



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

June 8, 2016

MS. ALEXA O'BRIEN
MUCKROCK NEWS
DEPT MR 17650
POST OFFICE BOX 55819
BOSTON, MA 02205-5819

FOIPA Request No.: 1329073-000
Subject: Carnivore

Dear Ms. O'Brien:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed is one CD containing 605 pages of previously processed documents and a copy of the Explanation of Exemptions. Please be advised, these are the only copies of these documents located in our possession. The original copies of these documents could not be located for reprocessing.

Additional records potentially responsive to your subject exist. The Federal Bureau of Investigation (FBI) has located approximately 1,594 pages total of records potentially responsive to the subject of your request. By DOJ regulation, the FBI notifies requesters when anticipated fees exceed \$25.00.

If all potentially responsive pages are released on CD, you will owe \$40.00 in duplication fees (3 CDs at \$15.00 each, less \$5.00 credit for the first CD). Releases are made on CD unless otherwise requested. Each CD contains approximately 500 reviewed pages per release. The 500 page estimate is based on our business practice of processing complex cases in segments.

Should you request that the release be made in paper, you will owe \$79.70 based on a duplication fee of five cents per page. See 28 CFR §16.10 and 16.49.

If you agree to receive all responsive material on CD, you will receive a \$5.00 credit towards your first interim CD. As a result, we must notify you there will be a \$25.00 charge when the second interim release is made in this case. At that time you will be billed for the \$10.00 remaining from the \$15.00 free of the first release, as well as the \$15.00 duplication fee for the second release, for a total of \$25.00.

Please remember this is only an estimate, and some of the information may be withheld in full pursuant to FOIA/Privacy Act Exemptions(s). Also, some information may not be responsive to your subject. Thus, the actual charges could be less.

talking about.

And so in the context of this message, there's actually a very simple answer if we're talking about a pen register and we want to know the tos and froms, the origins and destinations, the numbers, if we're going to extrapolate pen registers onto the Internet, there actually is, sort of, a very simple answer at the top here about where this packet is coming from and where it's going to. It's that first address, which is the yellow address, 207226, which actually happens to translate into the computer at CDT that I was using. And then there's a destination address which is in red there, which is that 216 address that happens to be CDT's mail server.

And that, if you just took it on its face, would be the very simple header information -- the numbers of the address that it's coming from, the address that it's going to.

What we're hearing about **Carnivore** is actually **Carnivore's** trying to do something a little bit more subtle, trying to get more information. The problem is, this is kind of difficult on the Internet because origin and destination is very context-dependent. It depends on where you are on the network, and what level of the protocol step -- what you're trying to do within the -- where you're looking within the packet.

And so in this case, it's an e-mail message. And you can see that the content of the e-mail message includes the line, "to Paul Taylor, mail that has come from Alan Davidson." That's the to and from information that the **FBI** is seeking to get. And so what **Carnivore** really needs to do is dig in to the content of this packet, analyze it, and ferret out this to and from information which is what the **FBI** says they want to get.

And I raise that just because, to think that this is a simple thing; to think that this is just information that's sitting on the top here and we can just pull off, is not to get the concept here. I think it's a very subtle thing, it's a very difficult thing, and it requires a lot of analysis.

Let's just skip real quick to that -- well, there's a second example which is an example of Chairman Canady's web site -- a similar situation. There's a to and from IP address at the top, but to actually get a look at what site I am visiting, what is the destination of this traffic, you have to look into the content of the packet. In this case, www.house.gov is the server, the host, and Canady p. 74 is the -- is the actual page that I was looking at at the time.

Now it's reassuring that the **FBI** says that they are not -- that **Carnivore** right now does not actually seek out URLs, the web sites that people are visiting, but if one's going to extrapolate this notion of numbers dialed into something that lets you get the origin and destination of Internet communications, it seems reasonable that this is the next thing they're going to look for.

And that becomes even more problematic. If you can go to the third slide, very quickly, I know I'm running out of time, this is a copy of a web packet. This is a web search that we do that looked at BarnesandNoble.com's web site. I did a search for a book -- this happened to be a book on prostate cancer, for no other reason than my personal interest -- someone in my family -- and I just wanted to show you what the URL looks like for this.

If the **FBI** continues this extrapolation and says, We just want to capture the URL, not the -- again the source and destination IP address at the top, but the URL of the web site destination that I'm visiting, they get a lot of information. They get this host in purple, which is shop@BarnesandNoble.com. They also get the page that I'm looking at, which is a book search, that is for prostate and cancer. You can imagine, this could be -- you know, I could be looking for all sorts of things. I could be looking for sites about religious

topics, or political topics, or social topics, and all of this gets listed in this pen register for the Internet.

And so, I think -- I realize I've gone over my time already here, but I think the point that I'd like to try to make is that, you know, some of these things, these rules that we've come up with, like pen registers, we came up with in the old context, the telephone context, for example. And the idea that digits dialed were something -- was something that wasn't as sensitive as what drove, I think, Congress to create this extremely low standard for access.

DAVIDSON: And I think Congressman Nadler's really on to something when he questions what the standards are. There's a very big difference between a reasonable -- I mean a relevant standard and a probable cause standard in the pen-register context.

And I think there's a greater example -- so, when we talk about Carnivore, we've got a lot of concerns about how it's being used. I would just summarize to say we are concerned about the fact that it needs to be opened up for the world to see. There needs to be an open source methodology used here so that we know exactly which pieces of the packet Carnivore is looking at and how it's doing its searches.

Second of all, we think that there ought to be a bit more control in the hands of the ISP. The ISPs are the people who are in the best position to do this balancing test.

And, finally, I think all of this points to the need for Congress to revisit some of these basic protections. The question of whether or not the pen register should be applied to the Internet is just the tip of the iceberg. The home has exploded; there's all sorts of information that used to be kept in the desk drawer that's now being kept out on the network. The law does not protect that information well. We need to revisit this.

The White House has taken a good first step. We're looking forward to working with everybody. That step doesn't quite go far enough, but we really want to work with folks to try and improve the privacy protections here.

Thank you very much for your indulgence.

CANADY: Thank you, Mr. Davidson.

Mr. Perrine?

PERRINE: Mr. Chairman and members of the subcommittee, thank you for inviting me to testify on the subject of Carnivore and the Fourth Amendment. I believe that the current debate over the FBI's new digital wiretap tool commonly known as Carnivore is really about the risks in attempting to simply translate the policies, law and practices of telephone wiretaps to the digital realm of the Internet.

Today's testimony has shown over and over again that there are -- that these differing interpretations of old law, as applied to the Internet, may be leading to problems.

The debate should not be about this specific program. The real issue is how the government is attempting to extend its lawful access to the Internet. In the process of applying old laws to the new media, the

privacy of citizens may be eroded in ways not intended or permitted under current wiretap laws.

In my career in computer security, I've always been an advocate of personal privacy, unrestricted access to strong encryption and less government oversight and intervention in the lives of law-abiding citizens. Due to my work at the Super Computer Center, I also understand the need of law enforcement to be able to intercept traffic. We spend an awful lot of time detecting, analyzing and tracing computer intrusions.

But this is about balance. The needs of law enforcement and privacy are not mutually exclusive. There can be a balance between them.

Earlier this year, while I was visiting the FBI to discuss critical infrastructure vulnerabilities, I was invited to see Carnivore, although we didn't know it by that name. In technical terms, Carnivore is a high-speed packet sniffer with very aggressive filtering capabilities. It does examine all of the data packets passing through a network and filters out the data that does not meet its filtering criteria. This is very similar to tools that are already available in private hands. Every network administrator uses a packet sniffer in diagnosing problems. Carnivore has new functions in the way that it can aggressively filter and perhaps in the speed of the networks that it can monitor.

Carnivore does not appear to be a monitoring infrastructure -- and someone did use the word Echelon -- capable of real-time monitoring of large numbers of phone calls. It does appear, on its face, to be a tool specifically designed to meet the rigid requirements of a Title III wiretap order or pen-register order.

Recent news stories have compared Carnivore to a trunk-side wiretap, which is monitoring system that allows monitoring all communications running through a phone office, just to find the calls related to a suspect. Congress rejected the use of trunk-side wiretaps more than 30 years ago because they mix communications of the innocent with those of suspects. This is an interesting comparison, but may be flawed. Carnivore does at a fundamental level intercept and examine all Internet traffic, but it only does that in order to select or reject data based on its filtering rules.

The question comes down to at what point has an examination and the privacy violation actually occurred? Does the examination and the privacy violation occur if a program compares the intercepted data with its filter and then rejects the data, or does the examination not truly occur until the data's seen by a human being or if this is stored for later processing?

This also comes into play -- this trying to use an analogy of the old telephonic system into the Internet -- we've talked a lot today about pen registers, which the purpose is to require -- to acquire the phone numbers used. And we've also heard testimony that that is functionally equivalent to the to and from e-mail addresses. Are they the same? Actually, I think not.

But Carnivore is just a tool and its capabilities must be considered in the context of how it could be used. Carnivore, with no filters, appears to be capable of gathering all of the information passing through the network that it monitors. There's nothing to stop a person from Carnivore technically -- using Carnivore to monitor all the network traffic passing through an Internet service provider if they had the capacity. There's no way for anyone to know the configuration of the filters in a Carnivore system at the time that it's installed or the true capabilities of Carnivore without examining the source code of the system during installation and the filters during the monitoring process.

The ACLU and others have called for publication of the source code of the Carnivore system and their arguments are compelling.

PERRINE: However, a one-time publication or review of the source code, even by an independent verification validation organization, would provide only a snapshot of Carnivore's capabilities, with no assurances that the Carnivore program actually installed on an ISP was built from the sources that was reviewed.

Carnivore is also under constant development, so the source code snapshot that was reviewed would be out of date within a few weeks. So unless you're planning on having an ongoing independent verification validation process, you'll never know that what was installed was actually what was reviewed. And there is no source code review that would indicate the filters that were installed in Carnivore at a given ISP on a given case.

So, in conclusion, Carnivore does appear to be both a trunk-side wiretap and an attempt to bring limited wiretap capabilities to the Internet. It does have long-term implications for privacy that must be carefully considered. Old laws often breakdown when applied to the Internet, and I think we've seen that today. And applying these old laws, may unintentionally erode constitutional protections in unintended ways.

Law enforcement may need appropriate legal access to Internet communications under limited circumstances, but this access must be properly controlled and monitored to ensure that constitutional safeguards are maintained.

Thank you.

CANADY: Thank you.

Mr. Corn-Revere?

CORN-REVERE: Chairman Canady and members of the committee, thank you for inviting me back to testify on this important topic.

Rather than try to paraphrase my written submission in five minutes or so, I'll dispense with that and just try to address some of the points about Carnivore that were discussed in the testimony of the government witnesses. I'll just try and touch on two or three points related to what, in my experience, was Carnivore in its natural habitat.

One of the first points that was made is that Carnivore is used in only very limited ways; that it's used only when an Internet service provider either cannot or will not comply with a court order.

In fact, Mr. Painter testified that in the one challenge that he's aware of, that incoming e-mail addresses, but not outgoing e-mail addresses were received, that then required the government to move forward with the installation of Carnivore. That's not quite what happened in that case.

In the case in which I was involved, the ISP did try to comply with a lawful court order, the pen-register and trap-and-trace order. It's simply taken as a given, the ISPs are obligated, under the terms of the Electronic Communication Privacy Act, to comply with lawful orders of the -- lawful court orders to provide information, but at the same time, they're required to protect the privacy of their subscribers.

In this case, the solution that the ISP put in place did get all of the outgoing -- excuse me -- all of the incoming e-mail addresses, and it did supply a smaller number of outgoing e-mail addresses to the government. They were dissatisfied with that, saying there must have been more outgoing e-mail addresses.

In fact, we tried to explain, that they're any number of reasons why there may be fewer outgoing e-mails, then there were incoming e-mails. For example, the target of the investigation might have used a web-based e-mail source, rather than using his own resident program. But nonetheless, the U.S. marshals were dissatisfied with that solution and informed the ISP that they were coming to install Carnivore within two days. That's what prompted the court action that led to the magistrate's order.

I believe, Mr. Painter then testified that, since that time the ISP has provided excellent cooperation.

In fact, the ISP has done in subsequent cases what it did in that case. It provided and offered to provide ways to comply with orders that it received in ways short of installing Carnivore, and since that time Carnivore has not been reinstalled on its system.

Secondly, in response to a question from the chairman, one of the government witnesses suggested that it was the ISP and its implementation and not the Carnivore program itself that caused a crash and disrupted the ISP's system.

In fact, our experience was that Carnivore was incompatible with this system, requiring the ISP to make adjustments which led to a number of problems, that ultimately led to Carnivore being taken out, and then the next day the order for its installation expiring.

Let me say just one other thing about that order. In fact, there was a magistrate's order, still under seal, that did require the installation of Carnivore.

CORN-REVERE: We tried to work out in the terms of that order what safeguards we could to make sure that no more information could be collected than necessary. But, in fact, what the magistrate said in that order was that he would welcome the decision on the legality of Carnivore under the existing legal scheme to be decided by a reviewing court. We haven't had that kind of legal review yet, and I don't know of a case in which that may occur.

Next, the government witness talked about the number of safeguards that exist to make sure that Carnivore does not lead to excessive violations of subscriber privacy. For example, Dr. Kerr testified that the filter will ensure that Carnivore acquires only the information that is authorized by a court order and suggested that it would be necessary to obtain the assistance of a technician or even perhaps the assistance of the ISP to alter the programming of Carnivore so that a rogue agent might gain information to which he or she is not entitled.

I'm not a technician, so I can't really address that point, but I can say that in the case that I was involved in, I was told that Carnivore would be accessible remotely by government agents and that the configuration of Carnivore could be changed with the flip of a switch. Maybe that's correct, maybe it's incorrect, I don't know. It does suggest, perhaps, that the proposals that have been discussed earlier for independent review of Carnivore really are in order.

Next, we're told that we will be protected from invasions of privacy because there is an audit trail that makes sure that the filter is correctly set to correspond to what is authorized by the court order and that that will be available with the evidence in a prosecution. But in fact that's a safeguard that exists only if there is a prosecution, and the safeguards that exist under the law primarily exist for Title III interception orders, not for trap-and-trace orders.

There is no requirement to notify the target of a surveillance in a trap-and-trace situation that that surveillance took place. So if -- there's no way to ensure accountability in that circumstances.

As I had mentioned in my April 6 testimony, surveillance was undertaken briefly with **Carnivore** pursuant to a trap-and-trace authorization, which, as many people have noted here today, is available only with a showing of relevance -- certification of relevance by a law enforcement authority; there is no requirement of probable cause necessary.

I believe Congressman Bachus asked whether or not **Carnivore** has been used for violations of any other laws, such as antitrust laws or consumer protection laws or anything else. The response was given that **Carnivore** can only be used in the event that there are specified federal felonies as set out in Title III.

As a matter of fact, that's true only for Title III intercept orders. You're not required -- or you're not limited in the use of **Carnivore**, in the event that it's being implemented in response to a trap-and-trace order, to the felonies that are specified in Title III. All that has to be shown is a certification that the prosecutor or the law enforcement agent involved believes that the use of **Carnivore** would be relevant and the information gained would be relevant to an ongoing criminal investigation.

The rest of what I have to say is really just paraphrasing what I've written down and that's already submitted. And I'll just leave it at that and be happy to answer your questions later.

CANADY: Thank you, Mr. Corn-Revere.

Mr. Blaze?

BLAZE: Thank you, Mr. Chairman.

I should point out that my comments here don't necessarily represent the viewpoint of my employer. I'm here, so to speak, on my lunch hour to provide the scientific and technical perspective.

My interest in the problem of intercepting traffic on the Internet for analysis dates back to my doctoral work, where I built a system to collect traffic that I would analyze as part of my dissertation work. What I discovered then, and what's certainly become even more the case as we've gone to higher speed and more complex kinds of networks with more protocols running on top of them, is that the problem of collecting data from Internet packets, from the packet level, is a very subtle and difficult one.

BLAZE: So my comments today address the question not of how do we ensure against the possibility of malice or misdeeds on the part of law enforcement, but starting from the premise that everybody is acting with good will and honest -- and perfectly honestly, even still it's difficult to be sure that the tools being

used to collect information from packets, in the way Carnivore does, are behaving faithfully and reliably.

In particular, there is a strong possibility that omissions of collected data or garbling of collected data could cause misleading results that could put information collected out of context, or collect data inadvertently that should be attributed to another source or destination than it may initially appear.

There is no systematic way, unfortunately -- we in the computer security community learned this over and over again, these are hard-won lessons -- there's no systematic way to deal with large complex systems of software, particularly when the function of the software is security-critical. Certainly, Carnivore is a security-critical function.

One of the particular difficulties of managing complex secure systems is that very often they fail silently. They fail in a way that leads the observer to believe that they're working properly, but, in fact, subtle bugs mean that there are vulnerabilities or mistakes there anyway.

So we have the problem of being concerned with the reliability of data collected by a complex piece of analysis software, and the problem of ensuring that something connected deep within the infrastructure of an Internet service provider isn't itself vulnerable to external tampering or could itself be -- have control taken over by a malicious third party who is able to get access to it by exploiting some bug.

There're two ways that we stumble along in trying to assure ourselves that complex systems that we want to rely on are, in fact, trustworthy. One is by focused review by experts by audits, and I certainly want to strongly advocate that the kind of focused review by independent experts that was discussed in the first panel be done. But there are limits to what a limited set of experts can ever discover. We discover again and again that even after a security audit, new information comes out about the environment in which the software may be used or something may have been missed by the panel of experts that could only be known by widespread publication of the source code and details of the architecture of the system.

The security community, pretty much unanimously, supports the idea that source code should be published for any system that performs a vital security critical function. And I think the Carnivore system is a very good example of this.

Now, one of the objections raised to doing this in the case of Carnivore is that it might provide aid and comfort to the targets of investigations, who might find ways to circumvent the system. I think, in the case of Carnivore, the existence -- the mere existence and the architectural details of the Carnivore system don't really provide much help to the -- to someone who wants to evade it. It's very much like knowing the details of how a tape recorder works doesn't help you know that there's actually a microphone that's been installed in your apartment.

Instead the important information that a criminal would be interested in are the details of whether or not Carnivore has been installed in a particular place.

BLAZE: And, of course, no one advocates publishing the details -- the operational details of specific Carnivore installations.

So, in summary, I recommend that we -- that neither -- that while neither focused review by independent experts nor publication of source code are panaceas and ensure against any possible problem or abuse,

these are essential steps -- widely recognized essential steps that certainly should be done in this case. And I hope that will happen.

Thank you.

CANADY: Thank you, Mr. Blaze.

Mr. Baker?

BAKER: I've been on both sides of some of these debates. And I have to say I see both sides of this one. I think in some ways, both sides of this debate are stuck in a -- in the telephone world. A lot of the witnesses, some of the questions, suggest that maybe we could solve this problem by having ISPs take responsibility for doing these intercepts themselves.

And actually I think the FBI has got this about right. If the ISP wants to do it, then they should do it. But if you take an ISP -- a small ISP, and tell them, "You have to do it," they're going to treat this like an expensive unfunded mandate. And there's no reason why they're going to do it more enthusiastically or more privacy-protectively than the FBI. In fact, there's going to be less oversight.

This is not the phone company that could just hire somebody to do the wiretaps every day and add it to the rate base. They're not going to be doing what people saw the phone companies do by way of protection if they're small ISPs and they don't want to have this role. And I'll tell you there's plenty of ISPs that really don't want this role in spite of the noisier ones who do.

But I think the FBI and the Justice Department are also living in the past. To say you don't have an expectation of privacy in information that is in the hands of a third party in the Internet age is just crazy. I mean, our entire lives are in the hands of third parties.

To treat the to and from lines in e-mails as though they were just the same as the phone numbers that you dial is also bizarre. We know that the phone company collects those phone numbers because they send us a bill with those phone numbers every month. No one expects the ISP to be collecting our to and from lines, especially not the from line. They don't use the from line to deliver the message, you know. That's just content, and they should get a Title III order to collect it.

So if relying on the ISP doesn't work; if this really is a privacy problem, what should we be doing?

I guess I would say a couple of things. First, as Mr. Nadler suggested, we ought to be sending notice to people when they've been subjected to this kind of intrusion. We have a system right now that protects the privacy of the crooks, but not the innocent people who are investigated.

You know, if Mr. Davidson were under investigation -- he sent that e-mail to Mr. Taylor. The next step that the police would take would be to put a cover on all of Mr. Taylor's e-mails in and out. It's perfectly relevant to their investigation. They want to know whether he's also corresponding with other crooks that they're investigating. So they're going to have 60 days or 120 days of Mr. Taylor's in and out e-mail, just automatically. And he'll never know it, because he's not going to get indicted and get to see that information.

There ought to be notice. Only you guys can make that happen.

There ought to be oversight. The audit provisions, again, are very protective of crooks, but not of innocent people. The criminal defense attorneys are going to get to see this and they're going to be able to follow that audit trail, but Mr. Taylor, if his e-mail has been intercepted, isn't going to get a chance to see that audit. There needs to be somebody who will do that audit on behalf of ordinary citizens; we shouldn't be relying on criminal defense attorneys to do that for us.

Last point, if you want to do something about this, you probably ought to do it pretty quickly. That's because Carnivore's not the only way in which this is going to happen. The Communication Assistance of Law Enforcement Act had a provision that said, well, everybody has to provide trap-and-trace-capability. The FBI has said that means packet data carried by carriers has to have a trap-and-trace capability. The FCC has said, We're telling everybody, you've got to have something installed -- all you carriers have to have the capability of doing this trap-and-trace by September of 2001.

BAKER: We aren't going to tell you how to do it, but we're going to tell you you have to have it done by then.

There's only one -- well, there's two ways to do it: either let the FBI install Carnivore or you go out buy Carnivore on your own. I'm not sure those are really the only solutions that we want to have carriers have, but unless the FCC backs off of its deadline and its current mandate, that's what's going to happen and it'll be too late to install a lot of controls.

Thank you.

CANADY: Thank you, Mr. Baker.

And last, but not least, Mr. Sachs, and I apologize for not having more time for you there.

SACHS: That's OK. I'm going to be very brief in the interest of time.

My name is Peter Sachs, and I'm the president of ICONN. We're a small Internet service provider based in New Haven, Connecticut. And I believe I'm one of the small ISP that Mr. Baker may be referring to.

We do have the capability -- in fact, any ISP has the capability of supplying the FBI with exactly what it wants in a more accurate, more efficient and more private manner, because we have absolutely no need to look at anybody's information, except for the actual target.

FRANK: Mr. Chairman, could the witness speak up a little more, please?

SACHS: Any ISP can do this, in as little as two lines of programming code. It doesn't require any machine. It doesn't require any specialized programming skills, beyond the programming skills of a normal system engineer at an Internet service provider.

To confirm this statement, I asked my system engineer to set up a system to monitor all of my communications. And in less than hour he was able to see everything that was sent to me or from me on his machine in clear legible text. So there's no need for any specialized machine or any, sort of, specialized knowledge to be able to do this.

Carnivore also creates an extreme security risk for an ISP. To allow a third party to attach a computer, especially a secretive computer that's accessible from a remote location, to an Internet service provider is unheard of. It just provides any hacker out there with yet one other doorway into which they can enter your network, and essentially destroy your network along with all of the data of all of your customers.

Carnivore also presents a performance hit for an ISP. The moment you intercept all information flowing over an ISP's network, which is what Carnivore does, it causes a bottleneck. Bottlenecks cause slowdowns. As all of you know, the Internet is already slow as it is; slowing it down even further, doesn't help matters much.

Lastly, it may have a chilling effect on the information that my subscribers or any ISP subscriber sends over the Internet. If you're not going to send something because you're afraid of its content or perhaps just its destination, it raises very valid First Amendment concerns.

If the ISP gathers the data for the FBI under a court order, the FBI can't possibly see anything it's not supposed to see, because they're only getting what we give to them. If the FBI does the work, they at least have the ability to see anything they want, and they do, in fact, have the ability to see anything they want. The former method protects privacy and the latter method invites abuse.

Since the ISP can provide the ISP with exactly what it wants, without imposing upon the privacy rights of all the subscribers, why Carnivore? Why use the most intrusive means if the least intrusive means are readily available?

Thank you.

CANADY: Well, I want to thank all the members of this panel for your very helpful testimony.

I just have one question, related to Mr. Sachs' testimony. Mr. Sachs has testified that doing the interceptions or executing a trap- and-trace or pen-register order is a simple matter for any ISP; can be done in an hour, just a little programming and there it is. Now, that's not consistent with what the FBI has told us their understanding is.

And let me ask -- I guess maybe Mr. Blaze and Mr. Perrine would be two who might be in the best position to give me your take on whether it's closer to what Mr. Sachs says or exactly as Mr. Sachs says or what the FBI has had to say on that.

Is it as simple as -- and I'm not trying to be -- single out Mr. Sachs here, but that's a fundamental question for us to look at. Is it as simple from -- in your understanding as Mr. Sachs has presented it, or does he have a programmer that has special expertise that other ISPs might not have?

PERRINE: Well, I can address that from the standpoint of tracing computer intrusions and attempted

intrusions, I would say probably 30 to 50 percent of the ISPs that we contact don't keep much in the way of logs. We tend to deal with a lot of the smaller ISPs, we tend to see the same ISPs -- the problematic ISPs over and over again.

I think that it's fair to say that many ISPs could solve this problem if they were motivated to, but it's not a profit center. They aren't making money cleaning up or preventing computer intrusions at other facilities and they certainly aren't going to make any money providing information to the government.

PERRINE: They're not financially motivated to do it. Some of them have the technical capabilities, and I would have to say that there are some of them that do not.

CANADY: Mr. Blaze?

BLAZE: Sir, I'd just like to -- from a technical perspective, the answer is like most subtle, technical questions, it depends.

The problem with a system like Carnivore, from the point of view of complexity, is that it has to be general purpose; it has to work under a wide variety of operational conditions; and it has to work to collect a wide range of kinds of information, depending on what the court order is asking for.

Some ISPs may already have in their network, for example, logs of information. They may have, for example, port replication capabilities on switches that allow them, much more conveniently than an external tool, to collect the kind of data that Carnivore or a Carnivore-like system could only collect with some trouble and with some difficulty assuring yourself that it's operating correctly.

In other cases, there may not be the exact capability required, so, it depends.

PERRINE: If I could just add -- if the equivalent of Carnivore were available in open source, that would make the -- that would lower the barriers to entry for the smaller and less technically capable ISPs to provide this information.

And I think that this is something that is quite feasible. It's not a six-day project, it's not a six-year project, it's probably on the order of I think maybe three to nine months at the outside for the open source community to reproduce large parts of the Carnivore system. And that would make it easier for smaller ISPs to provide this information themselves.

DAVIDSON: Could I just jump...

CANADY: Mr. Davidson, sure.

DAVIDSON: Perhaps part of the problem in coming up with an answer is that we don't know exactly what Carnivore is doing. There seems to be a certain subtlety of analysis that the FBI is seeking. And perhaps the FBI's interpretation of what numbers dialed on a telephone is, in terms of extrapolating it to the Internet, might be different from what many of us would think it would be.

So we really -- it's hard to answer the question about whether ISPs can do what Carnivore does until we, sort of, know what Carnivore does.

CANADY: Well, I understand that. But I also understand the FBI's problem with making the source code publicly available if there are proprietary interests there. I mean, there are other people's rights that have to be taken into account if they've used proprietary information in developing that. So that's -- I don't know how you resolve that. It may be that you just develop another product that could be used in the way that Mr. Perrine described it.

I want to conclude my time by thanking all of you for your contributions. They have been very interesting. And I would -- I will also ask that you be open to receiving questions from the committee and responding in writing, if the committee sends you questions. That might help us as we complete the development of the record for the hearing. But we thank you very much.

And I recognize the gentleman from North Carolina, Mr. Watt.

WATT: Thank you, Mr. Chairman.

And in the interests of time, I'll try to be very brief, too. I've got two technical questions also.

Mr. Perrine mentioned the possibility of doing something similar to Carnivore on an open source basis. Am I mistaken that that would create a different set of problems? Wouldn't that, in effect, make the technology available to everybody? And you're not suggesting I walk in to Radio Shack and buy me a Carnivore system so I could tap into everybody's Internet?

PERRINE: Well, actually, I almost am. It turns out that Carnivore appears to be functionally similar to network sniffers that are actually shipped with commercial operating systems and free operating systems today. The special purpose -- or the special magic for Carnivore appears to be that it is capable of filtering out information in ways that other people haven't had an incentive to write a program to do it, and also that it can monitor higher speed networks. And I believe that that's probably where a large part of the proprietary code is in the very high speed monitoring.

PERRINE: And I believe that that's probably where a large part of the proprietary code is, is in the very high-speed monitoring.

But, as other people have mentioned, the idea is to neck all of the large pipes down to small pipes and then monitor those. And if the ISP can do that, then they don't need the ultra-high-speed monitoring capabilities.

And I think Matt has...

BLAZE: Yes. I addressed some of this in my written testimony. But the important point is that there's nothing sinister about the basic functionality of network sniffers. They're an essential tool, used by anyone who has to administer a network, such as an ISP or a local area network administrator. These tools are common place; they're widely available.

They may not have the -- they don't have the requirements for keeping the kinds of legal audit trails that a system like **Carnivore** would have. So the additional capabilities that something like **Carnivore** has don't provide additional interception capabilities, but rather provide these legal assurances and chains of evidence and audit trails that open source would benefit greatly from and that wouldn't provide any great aid to bad guys.

WATT: Mr. Baker, it looks like you...

BAKER: I have to say I think the **FBI** is right on this. If you publish exactly how you're filtering this, then people will try to write their e-mail addresses and spoof their e-mail addresses in ways to avoid that particular method.

It's really not the best idea to publish this. I think the likelihood that the public's -- the open source community is going to embrace **Carnivore** as a project is about zero. There are going to be very few benefits from doing that and a lot of costs.

WATT: Mr. Corn-Revere raised an issue that I want to not have him address because he's already acknowledged that he doesn't have the technical capacity to address it, but Mr. Blaze and Mr. Perrine and Mr. Davidson, maybe Mr. Sachs, Mr. Corn-Revere raised the prospect that **Carnivore** could be accessible remotely.

I think I understand what that means, that you could -- the **FBI** could sit in an office somewhere else and change the program and manipulate it from some remote location. That's what you intended, Mr. Corn-Revere?

CORN-REVERE: That's correct.

WATT: OK. Tell us whether that is technically feasible, since Mr. Corn-Revere doesn't know the answer to that, give me -- my technical experts can tell us...

PERRINE: Actually, I believe that is the case.

WATT: It can be remotely...

PERRINE: I believe that is the case. I had a very limited time to see it, but I believe that is true.

WATT: Mr. Blaze?

BLAZE: I should point out that the ability and necessity to be remotely controllable and configurable is precisely what we, in the computer security community, are made very nervous by. That capability potentially, if not implemented very, very carefully, could allow an external attacker -- third party -- to gain control of the system and potentially do quite a bit of damage.

WATT: Mr. Davidson, Mr. Sachs, if you'll address that same question quickly, I'll leave everybody else

alone.

SACHS: Sure. The remote accessibility is almost as bad as the invasion of privacy. Given the record of hacking of government web sites, which happens almost on a weekly basis, the fact that this secure Carnivore machine is going to be out there accessible remotely means any hacker can get into a system.

If they could get into the White House and hack that site, they can get into an ISP through Carnivore.

DAVIDSON: Changing the configurations remotely to the extent that it's possible, I mean, I think removes part of the check that we would hopefully think exists where an ISP at least is in some ways an intermediary of how the device is deployed. And so that raises another concern.

WATT: Thank you, Mr. Chairman.

CANADY: The gentleman's time has expired.

The gentleman from Alabama is recognized for five minutes.

BACHUS: Thank you.

Is there any rationale that any of you can think of why electronic mail or information traveling over the Internet should have less protection than, say, a person's telephone calls or their faxes or either their private mail?

SACHS: No. To the contrary, I think that in fact it should have at least as great a protection as we currently give to voice communications for example in Title III. There's a crying need, really, for the Congress to update the Electronic Communications Privacy Act to bring it into line with the expectation of privacy that I think that Mr. Nadler suggested and that most of us have.

These are, in many respects, our most important communications, involves our most sensitive data and our most private thoughts. And we do need to bring those into line.

The administration -- if I can for just a second -- the administration, I think partly in response to the Carnivore controversy, made some suggestions the other day. Mr. Podesta made some proposals. In my testimony, I've gone through those proposals in some detail. When you get a moment, I urge you to take a look at that.

But I want to stress this one point: Those proposals are not a solution to the Carnivore problem. Tweaking the surveillance laws, the wiretapping laws, doesn't get to the heart of the Carnivore problem, which is that it is a device that does allow the FBI to filter through, potentially to capture, huge volumes of communications, most of which are completely unrelated to the target of the investigation.

That's the real problem with Carnivore that the committee needs to address; Congress needs to address, I think by telling the FBI clearly, if it's not already clear in the statutes, that it doesn't have the authority to force a service provider to install a device like Carnivore.

BACHUS: Mr. Davidson?

DAVIDSON: In the interest of time, I'd just like to say, ditto. And add one point, which is that e-mail is really just the tip of the iceberg here.

I think that was part of the point I was trying to make is that the home has explored; things that we used to keep in our possession are now making their way out onto a network. And this is a trend that's only going to increase: finance records, health records, stock portfolios, information about your kids, all being stored somewhere else. Once it leaves your possession, the kind of protection it has under the law is greatly diminished. I think that's really the challenge here for this Congress, to think about how we deal with that.

BACHUS: I think Justice Brandeis predicted about 40 years ago that one day the government would be able to come into your home and basically determine everything you did and said. And I think maybe that day's arrived.

Anyone else wish to comment on that?

I read a question to the first panel which was that you can't go to the AT&T and say, We're going to analyze all the phone calls that go through your system. I mean, that's true, right? Can't do that. But isn't that what they're doing with ISP providers?

STEINHARDT: I think that's exactly what they're doing with an ISP provider. And it's not so much a technical issue, it's a legal issue. I think the FBI and law enforcement accepts it could not go to a telephone provider and install a Carnivore-like device, the kind that Mr. Perrine referred to. He said that was settled 30 years ago, and he's quite correct.

I think that the -- I think the legal basis for doing that to an Internet service provider is at least equally suspect, but it may take an act of Congress to clarify that point.

BACHUS: I think clearly the marketplace and technology has outrun the law, and in doing so has overrun our legal protections that have been in the law for years.

Let me ask you this: In your experiences, what procedures are typically followed to notify customers when information from Internet service providers and other companies about them is subpoenaed or requested by the government? Is there any notice?

BAKER: That's a very mixed bag. And it depends entirely on the policy of the ISP. Some ISPs have a policy of sending notice, others do not. There's no requirement one way or the other.

It seems to me that notice is a good idea. The government probably should be sending it, rather than relying on ISPs to say yes or no to notice.

BACHUS: It's my understanding that what they're saying is they don't have to give notice if there's a

reasonable expectation that if they gave notice the communications would stop. And I think in every case where they gave notice, it would be a reasonable expectation that the communications would stop, so.

DAVIDSON: You know, in some circumstances, we have delayed notice, and I think that that serves a very important purpose here, too. And I think there'll be circumstances where that's appropriate. At least then you know that this had happened, you have a chance to object to it, even if it's after the fact.

CANADY: The gentleman's time has expired.

The gentleman from Michigan, Mr. Conyers, is recognized.

CONYERS: Well, I begin by thanking this second panel, because this has served as a very important corrective for what we were just told for a couple hours earlier. And I'm sorry to hear that we ought to move very rapidly on this matter because the clock is running down on the 106th Congress. There's not much likelihood of that. But I'm hoping that this will prepare us for a much deeper investigation that we're going to have to indulge in.

Let me thank specifically, though, the American Civil Liberties Union, because they, in addition to this complex subject, work on a number of others that appear before the Judiciary Committee. And so I'm glad to see them working here as well.

Is there a feeling that we should probably try to require that notice be given to those who are the objects of a trap-and-trace measure, or is that getting a little bit too fine -- cutting too fine a line in the requirements on the Department of Justice?

Mr. Corn-Revere?

CORN-REVERE: Well, let me just address that question in the context of the previous one, and that is, in the case of an ongoing investigation, like with the trap-and-trace order, the ISP is expressly prohibited from providing notice. Otherwise if the target of the investigation knows that he or she is being investigated, then the communications will cease. So there's no notice before the fact.

I think it would be advisable at least to change the law so that anyone's who's been the target of a surveillance be notified after the fact, as currently is the case with respect to a Title III intercept order.

DAVIDSON: I would just add that I actually think that there are two more important things for trap-and-trace and pen registers, one of which is raising the standard which is extremely low right now for access to this information. The second is defining what trap-and-trace and pen register mean for the Internet.

As you see -- I mean, there's been this wild extrapolation of numbers dialed into somehow this, sort of, much more meaningful origin and destination of Internet communications. And I think that needs to be dealt with.

CORN-REVERE: If I -- if I could just add to that point, because Mr. DiGregory did cite the Supreme Court decisions finding that pen registers don't violate the Fourth Amendment if there's no warrant, because there's no reasonable expectation of privacy on that information.

If you actually go to those Supreme Court opinions -- and there are really two of them that address it, *Smith vs. Maryland* and *United States vs. New York Telephone Company*, it's important to read what the Court had in mind when it said that no privacy right was being invaded.

For example, in *New York Telephone Company*, the court said that a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed, a means of establishing communication. Neither the report of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed, is disclosed by pen registers.

Now obviously, that's very different from the kind of information that's acquired with respect to e-mail. Anyone who gets my e-mail address knows the identity of this party. It has my name in it. And that's true of many other people with e-mail. Certainly, if you're able to get URLs -- uniform resource locators -- for browsing on the Internet, that's the same as getting somebody's library record or the record of videotapes they have checked out.

CORN-REVERE: So, the kinds of information available on the Internet is completely different from what existed in the context of a pen register when the Supreme Court addressed those issues some 25 years ago.

STEINHARDT: If I could just add to that, first, Mr. Conyers, thank you for your price for the ACLU, I'll except that on behalf of the organization.

There's one other thing that I think the Congress needs to attend to, and that's the standard now for law enforcement to get access to stored records, which is extremely very low.

But as Mr. Nadler point out, people who expectations of privacy don't diminish by the fact that an Internet service provider may have, for an instant or perhaps a little longer, been holding those stored records. And we need to begin to treat those as the kinds of records which the FBI and other law enforcement agencies need probable cause in order to obtain.

CONYERS: Well, gentlemen, I see this attempt to bring into balance the tensions between the Department of Justice and the Constitution -- citizens' rights to be an enormous one. I see a complex, I see a changing, because, as new technology comes on -- are there any of you here that can give me any words of assurance that it may not be as big as it seems to be this afternoon? We probably need some...

(CROSSTALK)

CANADY: The gentleman's time has expired.

And the gentleman from Arkansas will be recognized.

HUTCHINSON: Thank you, Mr. Chairman.

And I was absent during some of this testimony, but I want to assure everyone that I've read your testimony and have a great interest in your viewpoint on it. And I think everybody here probably was present during the previous panel's testimony, and I'd just like to ask a general question to Mr. Davidson, perhaps Mr. Steinhardt.

Did both of you hear the testimony of the previous panel? I'd just like to ask a reaction as to -- I mean, from what I gathered from the first panel's testimony is that, first of all, everything through to the Carnivore program is proceeded by a court order.

The -- secondly, a concern is whether there should be some independent review of the source codes. And I think that's something I had a discussion with them on -- you know, they're submitting it to -- willing to spend an independent evaluation, I think there's a question whether there should be some type of ongoing review, but I think that's an issue that's out there.

And then, you know -- but I was asking questions that -- you know, they're retrieving information for the Carnivore program, not for purposes of expanding what they achieved -- or received, but to limit it and to minimize it. And so, if you could just comment on whether you disagree on any of those conclusions?

Mr. Davidson?

DAVIDSON: Let me start by saying, I think some of those things actually sound good. And I mean, I think the idea of trying to minimize information that's collected in a context of an Internet, you know, surveillance is a good thing.

I think the problem is we just don't -- A, we don't know, really we don't know how well it's going to be doing that. And we've got to have a chance to look under the hood and understand this. And I think courts are going to need an understanding and defendants are going to need to understand it, and people are going -- public needs to build some confidence in it.

HUTCHINSON: And how would you suggest doing that?

DAVIDSON: I think this notion of opening up the code, I think is a very good one. If there needs to be a preliminary step of getting an independent panel in here, that's not the same and it wouldn't be as good as opening it up to the public.

I think that -- personally, I think that any system that relies on -- if I can be so easily violated by somebody knowing how it works, then I don't think it can be that useful a system. If the bad guys can figure out, you know, how to evade it that easily, then, you know, how good can it be? And I think that -- I'm not convinced yet that opening it up is a bad idea. But maybe that's what we can get an independent group in here for.

I think, but, you know, from a greater point of view, there's, sort of, this -- the issue it raises is, there is this desire on the part, I think of law enforcement to be able to extrapolate every current capability, like pen registers or trap-and-trace orders, into the Internet world. The fact is, that when you do that, some of them don't translate very well.

Pen registers is probably the example we've talked about the most here. When you -- we don't know what

they mean in the Internet world when we try to extrapolate them, we get a lot more information...

(CROSSTALK)

HUTCHINSON: You suggest a higher standard for a pen register for Internet access?

DAVIDSON: Absolutely a higher standard and a clearer definition of what it means. But I think there's got to be an understanding that some things they're going to be able to do -- I mean, there are new capabilities that the FBI is getting all the time, because of the sea of information that's out there.

The Internet's a very good thing on some level for law enforcement. I think there's going to have to be a recognition that maybe some of the things they can do now they'll have to do differently in the future. It's not necessarily a horrible thing. There's going to be lots of new tools for law enforcement as well.

HUTCHINSON: Mr. Steinhardt?

STEINHARDT: Well, in my mind, the testimony from the government panel raised more questions than it answered. I mean, for example, the testimony, it seemed to me to suggest that the only thing that Carnivore is, at least at the moment, and I think the implication was to be primarily used was the interception of e-mail.

STEINHARDT: But we know from -- I know from those persons who have seen some of those demonstrations, for example, members of the press who have seen some of these demonstrations of Carnivore, that it is capable of analyzing and potentially intercepting far more than just e-mail. There are a whole range of Internet protocols which Carnivore is capable of filtering for. There was some allusion to those here today.

HUTCHINSON: Could I interrupt you here for a second?

STEINHARDT: Yes.

HUTCHINSON: I mean the government has that capability of doing unauthorized wiretaps. They have the capability of gathering more information than they're entitled to under a court order. It's the court order that restrains the use of gathering techniques. And so there's always consequences to that.

But I mean obviously any of these can be abused, and they could gather more information but they're limited by a court order.

STEINHARDT: No, no, perhaps I wasn't clear Congressman Hutchinson.

CANADY: I'm sorry, the gentleman -- if he could finish in 15 seconds, because we're -- we need to conclude. The gentleman's time has expired.

STEINHARDT: Well, the government witness, for example, suggested that they had one case -- had gotten files through the file transfer protocol. The committee didn't have an opportunity to get into that question, but I think there are serious question about whether or not existing law permits them to get that for example with a trap-and- trace order.

HUTCHINSON: Thank you.

CANADY: The gentleman's time has expired.

The gentleman from New York, Mr. Nadler, is recognized for five minutes.

NADLER: Thank you Mr. Chairman.

I have a series of questions. I hope the answers will be brief because of the time limitation.

Someone said before that the Carnivore system is kind of sniffer system, that there are many others out there. So, you could have a lot of private sniffers. How do you -- how would we -- if there a danger that private sniffers can get all sorts of information violating people's privacy and how would we know that it has happened?

BLAZE: Someone who wanted to use a commonly available sniffer program to violate some one's privacy, would still have the problem of getting access to the network over which that traffic flows. That's the hard part, getting the software to do the interception.

NADLER: That's what the FBI is asking us to let -- to mandate the ISPs to do in this case?

BLAZE: Right.

NADLER: OK. Thank you.

Secondly, we talked about the question of remote accessibility of the FBI -- of the Carnivore system. And someone mentioned that you could change the configurations remotely. Do I understand correctly that what is saying is that the FBI, or for that matter a hacker, could, by changing the configurations, could, in effect, change evidence and implicate somebody in some crime if they had a motivation to do that?

BLAZE: Well, the answer to that depends on the security of the remote access system. If its implemented in a secure manner, then the chances of that are very small. If it's implemented in an insecure manner, then the chances of that become quite great...

NADLER: Let's assume, let's assume that the police were under some -- we know that this has happened in the past -- the police were under some great pressure to solve some heinous crime and they figure they've got their guy and let's just give a little more evidence. Could they use the Carnivore system to, in effect, manufacture evidence?

BLAZE: That would depend on how the audits are implemented and that's one of the reasons that open review would be a very useful thing.

NADLER: So, the answer is yes, unless you put in safeguards to prevent it?

BLAZE: Yes, that's correct.

NADLER: OK, so we'd have to make very clear that.

Mr. Steinhardt, you have suggested that -- in your written testimony you say that ECPA the -- whatever that was -- I forget the acronym -- should be amended to require the trap-and-trace/pen- register orders shall only be issued on the basis of an independent finding by judicial officers if there is reasonable cause to believe that the target of the order has or is about to commit a crime. By reasonable cause, you mean the same thing as probable cause, or you mean something different?

STEINHARDT: Well, it a slightly lesser standard than probable cause.

NADLER: OK, now you are suggesting that trap-and-trace and pen- registers for the Internet should have this higher standard than this simply certification that it's relevant to an investigation.

STEINHARDT: Yes, we're suggesting two things. One now is simply a certification; the judge has no discretion to turn down the request. And secondly, that there ought to be a high standard. Probably cause is fine with us, but there ought to be a high standard before the court issues that order, because, as you pointed out, this is an area where people do have a reasonable expectation of privacy and ought to have a reasonable expectation.

NADLER: And you're suggesting that for the Internet. You're not suggesting that for telephones?

STEINHARDT: We believe -- no, we are suggesting that for the telephone context as well.

NADLER: Because you believe that even in the telephone conversation -- telephone context, rather, the expectation of privacy is more substantial than the Supreme Court seemed to think it was 25 years ago?

STEINHARDT: Yes, I think clearly it is, yes.

NADLER: Why do you say clearly it is?

STEINHARDT: Well, I think most people would be very surprised to learn that they don't have a reasonable expectation of privacy in the numbers they dial, and the persons who call them. I think that's common sense. I think the Supreme Court decision defies common sense.

NADLER: Mr. Baker wants to say something on this.

BAKER: Yes. If I could add to that, in the -- when the Supreme Court wrote 25 years ago, it might have been true that you couldn't tell whether the call was completed, what was said and the like. But in the course of CALEA, the FBI has forced on the industry an enormous amount of transactional data gathering about calls other than content, which now can be obtained through trap-and-trace orders: how long you talked, whether you were on call waiting or call conferencing.

NADLER: Whether it was completed at all.

BAKER: Who conferenced in and when they got off. All that information would be part of a trap-and-trace order today.

NADLER: On telephones today, which was not the case and may in fact -- so the Supreme Court, if it were the same judges, using the same reasoning, might come to a different decision today because the facts are different.

STEINHARDT: I think many of us would think that they would, even in a telephone context, certainly in the Internet context. And Congress independently can certainly raise the standards for these things. Congress set the standard for this independently of the court.

NADLER: Well, let me just say, since my time is expiring, I appreciate this panel in particular and I think that the Congress has to act because the history shows that police agencies cannot be afforded untrammelled discretion, and we cannot always assume their goodwill or even their lack of mistakes in protecting people's privacy.

CANADY: The gentleman's time has expired.

The gentleman from Georgia is recognized for five minutes.

BARR: Thank you, Mr. Chairman.

Mr. Sachs, is it correct to say that an Internet service provider -- if project Carnivore is forced on them, they have no control whatsoever over that program -- that device?

SACHS: That's my understanding, correct.

BARR: And no supervisory capability whatsoever?

SACHS: That's my understanding, correct.

BARR: Mr. Corn-Revere, did it surprise you, as I think it did -- I know it did me and I think it did Mr. Sachs also -- to have the government say that -- I think they said this, although they, of course, always waffle just a little bit -- that, in virtually every instance, the only reason for those 25 instances over the last two years in which they used project Carnivore was simply because the ISP provider refused to or could not satisfy them that they could provide the information they wanted in the way they wanted it?

CORN-REVERE: I have no idea what the government's experience was in those other 24 instances, but in the one example in which I was involved that certainly was not the case. The ISP did attempt to comply with the court order without the installation of Carnivore and ultimately was given no choice.

BARR: That's my impression, too.

If we could put back up on the board, Mr. Davidson, any one of your examples, and I'll come back to you in just a second.

But, Mr. Steinhardt, you're very familiar, and maybe some other members of the panel are also, with regard to a recent proposal by the government and by some of their colleagues up here in the House and the Senate to amend Fourth Amendment law, through amendments to a methamphetamine bill and the bankruptcy bill, to essentially carve out from the necessity for providing an inventory of seized items intangible information. Now, so far, knock on wood, we've been successful in stopping that from moving forward.

Is this the sort of data that the government would consider intangible so that they would, if they came in and seized it somehow, would not be required to tell you they've taken it?

STEINHARDT: Well, the capacity of the government to make creative arguments about what the law provides them in the way of investigatory tools never ceases to amaze me. So, yes, I think this is exactly the kind of information which they will make a claim is tangible and would be subject to those kinds of disclosures.

BARR: I would suspect so.

Mr. Davidson, with regard to your examples here, if you could just very briefly -- and this may be very elementary but I'm not familiar with all the details here -- which one is this? Example three. He went down to line 12 there that's in -- that's highlighted in, I guess, purple.

Are you saying that, in order for the government to get in and get that information, if that information is the target of what they're authorized to receive or on any e-mail they have to get in there to see if it is or it is not, that that means that they would also have to necessarily in every instance look at items one through 11?

DAVIDSON: Well, again, I think it's difficult to know exactly how their system works. It could be quite sophisticated. And there's a lot of -- well, the answer is, I think again, it depends.

DAVIDSON: They may be able to extrapolate from certain pieces of lines one through 11 what lines they need to look at in order to find this information. Again, this one is in the context of a communication with a web site.

But, yes, I think my general point was that they need to look at a fair amount of this packet in order to do the analysis to figure out what it is that they're entitled to.

BARR: Otherwise, there's no purpose to having Carnivore?

DAVIDSON: Exactly.

BARR: I mean, if Carnivore just sat there, fat, dumb and happy, and just waited for stuff to fall into its lap, it would never get anything. I mean, it has to go in there and look at this stuff somehow, doesn't it?

DAVIDSON: Right. And I think that there is a big question about whether or not that is a search in and of itself. There's a separate, sort of, kind of technical question, which is just to show how difficult this is and why we need to have some kind of real oversight, because there is all this investigation going on.

BARR: But would everybody agree that at this time, at least at this point, we need to probe further? We know so little about this and the ramifications and potential for abuse are so great, that -- and I forget who it was, that, sort of, times a wasting and we need to get in here and look at this to see exactly what it is, so that we can determine to what extent we need to refashion these, you know, very outdated laws.

DAVIDSON: I think that we would ask that Carnivore, you know, not be deployed without further, you know, public oversight and information about what's going on there. At the very least, some sort of independent review panel as a start.

BARR: To at least maintain the status quo without -- the pre- Carnivore status quo.

DAVIDSON: It's problematic enough.

BARR: Thank you.

CANADY: The gentleman's time is expired.

I want to thank all the members of this panel, again. And all the members of the subcommittee for your participation today. The testimony of the witnesses has been very helpful to us.

The subcommittee will stand in brief recess. This hearing has concluded.

END

NOTES:

Unknown - Indicates speaker unknown.

Inaudible - Could not make out what was being said.

off mike - Indicates could not make out what was being said.

LANGUAGE: ENGLISH

PERSON: CHARLES T CANADY (94%); HENRY J HYDE (72%); SPENCER THOMAS BACHUS (57%); LINDSEY GRAHAM (55%); BARNEY FRANK (54%); JOHN CONYERS JR (54%); MAXINE WATERS (54%); DAVID GREEN (53%); JERROLD NADLER (53%);

LOAD-DATE: July 27, 2000

FOCUSTM

Search: General News; FBI and Carnivore

To narrow this search, please enter a word or phrase:

Example: House of Representatives

FOCUS

About LEXIS-NEXIS | Terms and Conditions | What's New
Copyright © 2000 LEXIS-NEXIS Group. All rights reserved.

FBI Is Pressured To Disclose Codes For Carnivore

DATE 7-24-00
PAGE 46

By TED BRUNS

Staff Reporter of THE WALL STREET JOURNAL

WASHINGTON—The Federal Bureau of Investigation is under increasing pressure to disclose the secret blueprints for its Carnivore surveillance system so independent technical experts can verify that the software monitors only the Internet communications of criminal suspects.

Despite mounting calls to permit such reviews, FBI officials maintain that disclosing the software's source code would allow hackers to find ways to defeat the system. The officials also argue that such a disclosure could violate copyright protections because Carnivore includes portions of software code from a product licensed to the government by an unidentified vendor.

Congress is expected to press senior FBI officials on the subject at a hearing today before a House Judiciary Committee panel led by Florida Republican Rep. Charles T. Canady. Lawmakers have indicated that they would seek assurances from the bureau that e-mails from innocent citizens aren't gobbled up whenever a federal judge agrees that the FBI can plug Carnivore into an Internet service provider's network.

One scheduled witness for the hearing, Matthew Blaze, an AT&T Corp. researcher, says the FBI's failure to fully disclose how Carnivore works has contributed to an "atmosphere of mistrust and confusion."

In an essay published on the Internet last week, Mr. Blaze wrote that releasing the system's source code "is a critical first step in assuring the public that Carnivore can at least be configured to do what it is supposed to do." Mr. Blaze questioned Carnivore's effectiveness, suggesting that even modest electronic forgery or data-scrambling techniques could foil it, and described conditions under which it could mistakenly capture e-mails and other communications intended for innocent users.

While the FBI is resisting calls for broad disclosure of the source code—already the target of at least two requests under the Freedom of Information Act—the bureau has sought to assuage fears by describing in remarkable detail how the system works. On Friday, dozens of reporters crowded a conference room at FBI headquarters to watch a demonstration.

The bureau has also proposed a compromise, tentatively agreeing to an examination of Carnivore by university researchers who would promise not to disclose its blueprints.

The American Civil Liberties Union, one of the groups that has requested the source code, said it might agree to such an offer if the FBI gives the blueprints to the ACLU and lets it select the experts.

USA TODAY

Today's debate: FBI and Internet privacy

FBI eavesdrops on e-mail, crashes privacy barriers

Our view:

Agency says it targets criminals. History says it can't be trusted.

The FBI has a knack for concocting colorful code names for crime-busting toys. The latest is "Carnivore" — an eavesdropping device that devours private e-mail and spits out interesting parts for scrutiny. Not just criminals' e-mail. Anyone's e-mail.

The FBI already has attached Carnivore to the e-mail hardware at some Internet service providers. Though it won't say where, the FBI says the tool has been used fewer than 25 times. Once it's in place, Carnivore acts as an unrestrained Internet wiretap, snooping through every Internet communication that comes within its reach.

The House Judiciary Committee will hold a hearing today, at which it will ask the FBI to explain its actions. But in the 15 weeks since Carnivore was revealed in obscure congressional testimony, the bureau has evaded answers about both its capabilities and proposed uses. The bureau won't answer even the most basic questions about whom the technology targets and how it protects the privacy of innocent Internet users. The potential for abuse is unprecedented:

► **Who.** Carnivore is intended to rifle through potential criminals' Internet traffic after police obtain a court order. But the tool gives the FBI the ability to track not just the individual named in the court order, but also everyone who uses the same server at the Internet service provider. At America Online, for example, that would be thousands of people. What's to keep the FBI from snooping more broadly? Only its own assurances.

► **What.** Coverage so far has focused on the surveillance of e-mail, but a program that can snoop through e-mail can just as easily eavesdrop on Web surfing, since the information travels in similar forms over the same servers. What information will the FBI collect about the sites people visit and even the ads they click on?

► **When.** The FBI admits that Carnivore is more invasive than a conventional phone tap. Yet it faces no more restraints than those that protect telephone conversations, which are themselves inadequate. Since Carnivore is a greater threat to privacy, shouldn't there be more restrictions on when it's used?

► **Why.** The Congressional testimony that revealed the existence of Carnivore also disclosed two other systems used by the FBI for similar purposes: "Omnivore" and "Ether-peek." Why weren't those revealed earlier? How many times have they been used and for what purpose?

The FBI's response to those questions is, in essence, trust us; we're only after criminals and terrorists. But even a cursory glance at law-enforcement history shows that promise can't be trusted. The temptation of government to collect and misuse information is irresistible. (See box.)

Further, the FBI shows no inclination to exercise restraint. In every aspect of electronic privacy — computers, the Internet and cellphones — it has pushed invasiveness to the technological limit:

► In 1994, the FBI lobbied to have backdoor access installed in every new computer to ease electronic snooping, allowing the FBI to defeat security. The plan was dropped after the National Academy of Sciences determined such access would make all computers more vulnerable to illegal break-ins.

► In 1995, the bureau asked for the capability to tap as many as one in 100 phones in major cities. It backed off only after a public outcry. Lacking such technology, no totalitarian state in the world is that invasive.

► In 1996, the FBI proposed liberalizing the export of encryption programs, but only for companies that, under court order, make available "keys" to defeat the privacy programs. After two federal courts struck down the proposal, the administration gave up.

► In 1997, the FBI went to court to protect a plan that would allow cellphones to be used by police to locate the positions of their users. The case remains in court today.

► Today, the thin answers the FBI has made public about Carnivore raise more disturbing questions. An explanation of Carnivore posted on the FBI's Web site casually discusses the electronic surveillance of an entire "facility," without explaining how broad such e-snooping could be.

In each case, the FBI gets convenience. The public gets government intrusion on a scale unequaled in constitutional history. Abuse will only expand as less-closely watched law enforcement agencies piggyback on the technology.

DATE 7-24-00

PAGE 16A

E-snooping grows

Court orders for America Online customer data:

1 — Estimate. As of July 2000, AOL had received more than 200 orders.
Sources: USA TODAY research; America Online

By Quin Tian, USA TODAY

FBI fumbles privacy

The FBI has a long history of violating the privacy of U.S. citizens, often with political motives. Some examples:

► 1956: The FBI rifled credit files and criminal records of 43 ordinary Delaware citizens called to jury duty in a politically sensitive case. Many also were investigated for ties to the NAACP.

► 1960s: FBI wiretapped Martin Luther King Jr. to gather damaging information on extramarital affairs.

► 1970: FBI sent damaging information on NAACP chief, Rev. Ralph Abernathy, to Vice President Spiro Agnew.

► 1980s and '90s: FBI kept a file on AIDS activist group ACT UP and its planned protests.

► 1993 and '94: The FBI "inadvertently" released files containing unsubstantiated allegations on numerous Republicans to low-level political appointees of the Clinton administration.

Attorney General Janet Reno said last week that she intends to begin a thorough review of Carnivore. That's a positive step, but it's hard to understand how Reno wouldn't already have a complete knowledge of the tool since she is the head of the "President's Working Group on Unlawful Conduct on the Internet," which just completed its report in March.

The Clinton administration greeted howls about Carnivore's reach with a proposal to update electronic-privacy laws, although congressional Democrats say the bill has no chance of even being voted on this year.

The time for such updating and review was before Carnivore was used. Carnivore needs to be shut down until an outside review of its capabilities and safeguards is complete. And the Internet companies that willingly complied with the FBI's use of the technology in the past need to come forward and inform individuals whose e-mail the FBI "filtered."

Of course, law enforcement agencies cannot operate without ways to monitor the modern communications tools of criminals. But even a cursory glance at the FBI's history shows it can't be trusted to make privacy for everyone else a priority.

The right of the innocent to be free from government intrusion should not be compromised to make life easier for the FBI. Until the bureau can show that its new technology poses no threat to the public, Carnivore needs a starvation diet.

Technology used narrowly

Opposing view:
Court order required to intercept only specific e-mails of criminals.

By John E. Collingwood

First, let's get the facts straight. The FBI and all other law enforcement agencies can intercept e-mails only pursuant to a court order signed by a judge who is satisfied that the government has demonstrated probable cause that a serious crime is being or has been committed, that the e-mails will be about that crime, and that the interception is necessary to obtain evidence about the crime.

Conducting an intercept beyond that is a federal crime subject to severe criminal and civil sanctions. The entire process requires continuous reporting to a court and, of course, ultimately is subject to vigorous challenge by defense attorneys. Even when only address information is sought, a court order is still required.

What does "Carnivore" do? In the simplest terms, it ensures that only the exact communications authorized by the court to be intercepted are intercepted. So, for example, if a court authorizes only the interception of e-mail from a particular drug dealer to another drug dealer, this system captures only that e-

mail to the exclusion of all other communications, regardless of whom sends them and where they are going. Nothing else is monitored or collected, and everything collected is supervised by the court.

When is Carnivore used? It is used only when an Internet service provider cannot, on its own, effect the interceptions consistent with a narrow court order. Accordingly, it has been used very few times, predominately in terrorism cases.

In 1968, Congress spelled out strict requirements for interceptions. Carnivore simply ensures that law enforcement agencies comply precisely with those requirements as technology advances. We understand why certain segments oppose this court-supervised technique. But since 1968, because of this law, many lives have been saved and thousands of drug dealers, terrorists, child predators and spies are in jail.

The chairman of PSINet laid out the appropriate challenge. He does not want to see Carnivore on his network unless we can prove it collects only the traffic from the target of a court order. That, of course, is precisely what Carnivore does, electronically protect the privacy of those not subject to the court order.

John E. Collingwood is an assistant director of the Federal Bureau of Investigation.

July 24, 2000

Mr. Brian Gallagher
Editor of the Editorial Page
USA Today
1000 Wilson Blvd.
Arlington, VA 22229

Dear Mr. Gallagher:

In response to today's editorial about "Carnivore," again let's get the facts correct.

USA Today rightly points out that "law enforcement agencies cannot operate without ways to monitor the modern communications tools of criminals" but then questions who should ensure that privacy is properly protected. The simple answer is the same as it has been for over 30 years--federal judges. All of the federal criminal and civil sanctions and judicial oversight that apply to wiretapping and have effectively protected those not the target of a court order apply to the use of Carnivore to intercept the e-mails of criminals.

Unlike as the editorial reflects, however, Carnivore does not snoop through every Internet communication, does not spit out everyone's e-mail, and is not an unrestrained Internet wiretap. Court orders authorizing the intercept of criminals' e-mails come only after rigorous review and the conclusion that there is probable cause that a crime is being or has been committed, the e-mails are about or in furtherance of that crime and the intercept is necessary to gather evidence about the crime. The orders are specific as to whom and what can be intercepted and then the courts supervise the interception to ensure compliance. Evading those court orders is a serious crime which would, of course, produce absolutely nothing of evidentiary value.

Finally, the editorial says the "Bureau won't answer even the most basic questions about whom the technology targets and how it protects the privacy of innocent users." Contrary to

1 - Mr. Pickard
1 - Dr. Kerr
① - Mr. Parkinson
1 - Mr. Collingwood
JEC:mmc (8)

1 - [REDACTED]
1 - [REDACTED]

66-1
67C-1

Mr. Brian Gallagher

that assertion, however, the FBI has shown the system to and answered these questions for dozens of people on Capitol Hill and over 30 reporters representing 25 media outlets. USA Today, of course, was invited and today we are anxious to present it at an open hearing before a congressional subcommittee. We are arranging for an independent review as well.

Sure Carnivore can be controversial and clearly is ill-named. But it is used only pursuant to court order; has been used sparingly, predominantly in terrorism cases, and then only when an Internet Service Provider cannot on its own comply with the court order; and, when used, collects only what the law authorizes and the courts instruct be collected--evidence about serious crime that cannot be otherwise gathered.

Sincerely yours,

John E. Collingwood
Assistant Director
Office of Public and
Congressional Affairs

Uproar worse than bite of this FBI beast

Carnivore might sound like a particularly violent computer game, or perhaps a movie that you wouldn't let your 12-year-old go see alone. It's actually a project of the FBI, which, depending on your outlook, is either a threat to the privacy of all Americans or a useful tool in fighting criminals.

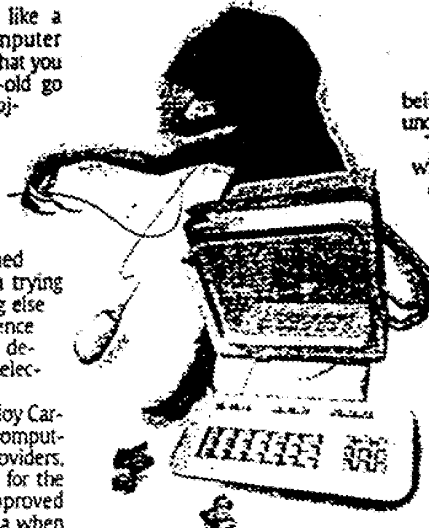
The unfortunately named program (the FBI has been trying to come up with something else since news of its existence broke) is an eavesdropping device housed in a tangle of electronics the size of a laptop.

The agency wants to deploy Carnivore boxes at the main computers of all Internet service providers, to provide an efficient way for the FBI to conduct court-approved wiretaps on e-mail in an era when all communication, lawful and otherwise, is going digital.

Since word of this hit during congressional testimony, the nation's privacy advocates have been outraged at the idea of the Internet being "bugged."

But it's not just activists who are up in arms. So is the Republican leadership in Congress. House Majority Leader Dick Armey of Texas has attacked Carnivore as being illegal under current wiretap laws, and the Constitution subcommittee of the House Judiciary Committee held hearings Monday to look into the matter.

Now, privacy advocates have



By Quinn Tamm, USA TODAY

been fighting for years to protect our information from prying eyes. But it's fascinating to see everyone else getting into such a lather over a system that — unless the FBI is lying through its teeth — is very limited in what it's allowed to do.

In a perfect world, I might be concerned about the idea that were I the subject of an investigation, the FBI could monitor my e-mail. But agents would at least have to go before a judge and get permission. And even at the height of government surveillance during the McCarthy era, the number of people

eLife

By Elizabeth Weise

being monitored numbered well under 1 million.

That pales in comparison with what's already happening with every keystroke we make as we wander the commercial Web.

Many sites record every search made and every mouse click, building up a detailed dossier of interests and surfing choices, which they use to target the ads that appear on our screens.

A fair number also "bug" their sites, scattering invisible cookies that our browsers pick up, allowing that site and others to share information to create an even more specific portrait.

In addition, by linking to outside databases, it's possible to attach that portrait to a name, address and personal data, including what stores you shop at, what you buy and when you pay your bills. And let's not forget that if the company goes out of business,

it can try to auction off its database to the highest bidder — though the government we so fear is working on making that illegal.

All that is bad enough, but it's nothing compared with what will happen when the Web goes wireless and we all begin accessing our e-mail, bank accounts and stock funds from cellphones. If you thought a cookie or two was intrusive, wait till everything you do is linked in real time to your phone number and exact physical location, as cellphones soon will be.

This isn't to say Carnivore shouldn't be carefully monitored or that we should trust the FBI just because it tells us to. I just don't understand why so many of the people up in arms over Carnivore rail against passing any kind of legal protection for consumer privacy online, saying the industry will develop only if it's left to self-regulate.

When it comes to the privacy of my personal information, I trust the government, which is bound by strict laws, a whole lot more than I trust multinational corporations.



DATE: 7-25-00
PAGE: 10-A

FBI defends e-mail surveillance tool

By Kevin Johnson
USA TODAY

WASHINGTON — Peppered with questions from skeptical lawmakers, the FBI played down concerns Monday that its e-mail surveillance program known as "Carnivore" could be used to eavesdrop on the innocent.

At a House Judiciary subcommittee hearing that seemed to capture both the promise and pitfalls of new technology for law enforcement, Assistant FBI Director Donald Kerr defended the program as a useful tool for agents. He said any surveillance done with the Carnivore program is limited to those suspects named in court orders.

Critics, including an unusual coalition of conservative Republicans and civil liberties advocates, have complained that the program could be used to do broad surveillance.

Their fear stems from the way

the FBI implements the Internet-wiretapping system. Carnivore works through a suspect's Internet service provider, such as America Online. It allows investigators to identify and view a suspect's e-mails among all e-mails moving through the provider's system.

Critics are concerned about giving law enforcement access to the e-mails of innocent people as well as suspects. Although Carnivore can retrieve any e-mails, investigators are restricted to those that have been approved for monitoring by a judge.

House Judiciary Committee Chairman Henry Hyde, R-Ill., said the Carnivore debate reflected an ongoing tension between law enforcement and individual rights.

"You can understand people's concerns for privacy? There are people who are skeptical about this culture of privacy and how porous it is," Hyde told Kerr and other FBI

officials at the House hearing.

Meanwhile, Rep. J.C. Watts, R-Okla., urged the Clinton administration to suspend the program, under which the FBI has intercepted e-mails in 25 probes over the past two years. No cases involving Carnivore have come to trial.

Justice Department officials also said they are reviewing the program to make sure that federal agents have not been involved in unlawful eavesdropping. Kerr said investigators involved in the Carnivore program have never been provided Internet traffic outside the scope of their probes: "We don't do broad searches (on Internet traffic) and surveillance that is not authorized by court order."

This year, the program has been used in 16 cases: six criminal probes and 10 national-security investigations.

July 25, 2000

Ms. Christine Bertelson
Editor of Editorial/Opinion Page
St. Louis Post Dispatch
900 North Tucker Blvd
St. Louis, MO 63101-1099

Dear Ms. Bertelson:

In response to your recent editorial "Silent cybercrime hunting," a few additional facts might help your readers understand the safeguards and judicial oversight applicable to the interception of e-mail on the Internet.

As always happens, dangerous criminals and terrorists use new technology as fast as anyone does. So now, instead of telephones, we increasingly find criminals communicating by e-mail in furtherance of their crimes. We have seen this in everything from child pornography to terrorism. That is why the FBI developed the Carnivore program, a tool that permits surgical interceptions in the midst of the flood of data on the Internet.

To use Carnivore to obtain a criminal's e-mail, the FBI first must successfully demonstrate to a judge that there is probable cause to believe that a serious crime is being or has been committed, the e-mails are about or in furtherance of that crime, and the interception is necessary to gather evidence about the crime. It is the same rigorous legal standard that applies to the interception of telephone conversations. The same severe criminal and civil sanctions apply to any misuse as well, and the whole process is supervised beginning to end by the federal court issuing the order. Finally, the use of this evidence and the method of collection are always subject to vigorous challenge by defense lawyers.

The FBI only uses Carnivore when an Internet Service Provider cannot, on its own, provide the very limited information authorized by courts to be intercepted, e.g., e-mails to and from two drug dealers. That is why it has only been used 25 times since it was developed and, in these cases, it was used with assistance from the Internet Service Provider.

1 - Mr. Pickard
1 - Dr. Kerr
① - Mr. Parkinson
1 - Mr. Collingwood
JEC:mmc (9)

1 [REDACTED] 66-1
1 [REDACTED] 670-1
1 [REDACTED]

Ms. Christine Bertelson

Finally, Carnivore does not "automatically" search for "key words among all e-mail traffic." It does not search the content of e-mail at all. To search as the editorial suggests would be contrary to federal law, subject to severe criminal sanctions and produce nothing of evidentiary value because it would contravene the parameters of the Fourth Amendment. Instead, Carnivore ensures that law enforcement only gets those specific e-mails addressed as described in the court's order to the complete exclusion of everything else on the Internet.

Sincerely yours,

John E. Collingwood
Assistant Director
Office of Public and
Congressional Affairs

(Mount Clipping in Space Below)

(Indicate page, name of newspaper, city and state.)

Editorial Page, St. Louis
Post Dispatch, St. Louis, Mo.Date: 7/24/2000
Edition: Final *****

Title:

Character:

or

Classification:

Submitting Office: St. Louis

Indexing:

PRIVACY

Silent cybercrime hunting

WITH a staggering 1.4 billion e-mails exchanged each day, Internet technology has raced around and ahead of laws governing traditional forms of communication and commerce. That is part of the Internet's appeal, but also part of its danger. Many of the 2.2 million Americans who talk and shop on-line were less than happy to hear that the Federal Bureau of Investigation has been using an e-mail patrol system with surveillance capabilities far beyond those of telephone wiretaps.

Most citizens feel reasonably comfortable with Fourth Amendment protections and laws that allow phone call traces and wiretaps of suspected criminals. But Internet communications are vulnerable in a different way. The FBI's "Carnivore" system, named for its ability to hunt down "meat," automatically searches for key words among all the e-mail traffic of a suspect's Internet service provider. That creates an enormous potential for abuse and loss of privacy.

The White House and Congress, ever late in chasing cyber-issues, are considering

legislative proposals to create Internet privacy protections comparable to those governing telephone conversations and the search and seizure of personal papers. But Internet communication — some along telephone lines, some along cable television wires — makes it a staggering task. A House judiciary subcommittee plans to hold hearings today to weigh law enforcement needs and constitutional privacy rights, and to examine the extent to which current laws let the government use devices like Carnivore.

The FBI says it has used Carnivore less than 50 times in the year it has been available, mostly to stalk suspected cases of hacking, intrusion and some counter-terrorism. Clearly, criminals can't be allowed to use the Internet as a safe haven for communications that authorities have been able to monitor for years on the telephone. But silent government sifting of the nation's e-mail is not acceptable. We urgently need new laws that protect citizens both from criminal suspects and invasions of privacy.



Department of Justice

STATEMENT
OF
KEVIN V. DI GREGORY
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
BEFORE THE
SUBCOMMITTEE ON THE CONSTITUTION
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES
CONCERNING
"CARNIVORE" AND THE FOURTH AMENDMENT
PRESENTED ON
JULY 24, 2000

STATEMENT OF
KEVIN V. Di GREGORY
DEPUTY ASSISTANT ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE
BEFORE THE SUBCOMMITTEE ON THE CONSTITUTION
OF THE HOUSE COMMITTEE ON THE JUDICIARY
on
"CARNIVORE" AND THE FOURTH AMENDMENT

July 24, 2000

Mr. Chairman and Members of the Subcommittee, thank you for allowing me this opportunity to testify about the law enforcement tool "Carnivore" and the Fourth Amendment. On April 6, 2000, I had the privilege of testifying before you during a hearing on Internet privacy and the Fourth Amendment; I am pleased to continue to participate in the discussion today about "Carnivore" and its role in protecting individual privacy on the Internet from unwarranted governmental intrusion, and about the critical role the Department plays to ensure that the Internet is a safe and secure place.

Privacy and Public Safety

It is beyond dispute that the Fourth Amendment protects the rights of Americans while they work and play on the Internet just as it does in the physical world. The goal is a long-honored and noble one: to preserve our privacy while protecting the safety of our citizens. Our founding fathers recognized that in order for our democratic society to remain safe and our liberty intact, law enforcement must have the ability to investigate, apprehend and prosecute people for criminal conduct. At the same time, however, our founding fathers held in disdain the government's disregard and abuse of privacy in England. The founders of this nation adopted the Fourth Amendment to address the tension that can at times arise between privacy and public

safety. Under the Fourth Amendment, the government must demonstrate probable cause before obtaining a warrant for a search, arrest, or other significant intrusion on privacy.

Congress and the courts have also recognized that lesser intrusions on privacy should be permitted under a less exacting threshold. The Electronic Communications Privacy Act ("ECPA") establishes a three-tier system by which the government can obtain stored information from electronic communication service providers. In general, the government needs a search warrant to obtain the content of unretrieved communications (like e-mail), a court order to obtain transactional records, and a subpoena to obtain information identifying the subscriber. *See* 18 U.S.C. §§ 2701-11.

In addition, in order to obtain source and destination information in real time, the government must obtain a "trap and trace" or "pen register" court order authorizing the recording of such information. *See* 18 U.S.C. 3121, *et seq.*

Because of the privacy values it protects, the wiretap statute, 18 U.S.C. §§ 2510-22, commonly known as Title III, places a higher burden on the real-time interception of oral, wire and electronic communications than the Fourth Amendment requires. In the absence of a statutory exception, the government needs a court order to wiretap communications. To obtain such an order, the government must show that normal investigative techniques for obtaining the information have or are likely to fail or are too dangerous, and that any interception will be conducted so as to ensure that the intrusion is minimized.

The safeguards for privacy represented by the Fourth Amendment and statutory restrictions on government access to information do not prevent effective law enforcement. Instead, they provide boundaries for law enforcement, clarifying what is acceptable evidence

gathering and what is not. At the same time, those who care deeply about protecting individual privacy must also acknowledge that law enforcement has a critical role to play in preserving privacy. When law enforcement investigates, successfully apprehends and prosecutes a criminal who has stolen a citizen's personal information from a computer system, for example, law enforcement is undeniably working to protect privacy and deter further privacy violations. The same is true when law enforcement apprehends a hacker who compromised the financial records of a bank customer.

As we move into the 21st century, we must ensure that the needs of privacy and public safety remain in balance and are appropriately reflected in the new and emerging technologies that are changing the face of communications. Although the primary mission of the Department of Justice is law enforcement, Attorney General Reno and the entire Department understand and share the legitimate concerns of all Americans with regard to personal privacy. The Department has been and will remain committed to protecting the privacy rights of individuals. We look forward to working with Congress and other concerned individuals to address these important matters in the months ahead.

Law Enforcement Tools in Cyberspace:

Although the Fourth Amendment is over two centuries old, the Internet as we know it is still in its infancy. The huge advances in the past ten years have changed forever the landscape of society, not just in America, but worldwide. The Internet has resulted in new and exciting ways for people to communicate, transfer information, engage in commerce, and expand their educational opportunities. These are but a few of the wonderful benefits of this rapidly changing technology. As has been the case with every major technological advance in our history,

however, we are seeing individuals and groups use this technology to commit criminal acts. As Deputy Attorney General Eric Holder told the Crime Subcommittee of this Committee in February, our vulnerability to computer crime is astonishingly high and threatens not only our financial well-being and our privacy, but also this nation's critical infrastructure.

Many of the crimes that we confront everyday in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft, and child pornography are migrating to the Internet. The Fourth Amendment and laws addressing privacy and public safety serve as a framework for law enforcement to respond to this new forum for criminal activity. If law enforcement fails properly to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cybercrime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is the key.

To satisfy our obligations to the public to enforce the laws and preserve the safety, we use the same sorts of investigative techniques and methods online as we do in the physical world, with the same careful attention to the strict constitutional, statutory, internal and court-ordered boundaries. Carnivore is simply an investigative tool that is used online only under narrowly defined circumstances, and only when authorized by law, to meet our responsibilities to the public.

To illustrate, law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products, or to whom the drug dealer is selling. To investigate this, it is helpful to determine who is communicating with the drug dealer. In the "olden days" of perhaps 10 years ago, the drug dealer would have communicated with his supplier and customers exclusively through use of telephones and pagers. Law enforcement would obtain an order from a court authorizing the installation of a "trap and trace" and a "pen register" device on the drug dealer's phone or pager, and either the telephone company or law enforcement would have installed these devices to comply with the court's order. Thereafter, the source and destination of his phone calls would have been recorded. This is information that courts have held is not protected by any reasonable expectation of privacy. Given the personal nature of this information, however, the law requires government to obtain an order under these circumstances. In this way, privacy is protected and law enforcement is able to investigate to protect the public.

Now, that same drug dealer may be just as likely to send an e-mail as call his confederates. When law enforcement uses a "trap and trace" or "pen register" in the online context, however, we have found that, at times, the Internet service provider has been unable or even unwilling to supply this information. Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet. We cannot do this without tools like Carnivore.

When a criminal uses e-mail to send a kidnaping demand, to buy and sell illegal drugs or to distribute child pornography, law enforcement needs to know to whom he is sending messages and from whom he receives them. To get this information, we obtain a court order, which we

serve on the appropriate service provider. Because of the nature of Internet communications, the addressing information (which does not include the content of the message) is often mixed in with a lot of other non-content data that we have no desire to gather. If the service provider can comply with the order and provide us with only the addressing information required by court order, it will do so and we will not employ Carnivore. If, however, the service provider is unwilling or unable to comply with the order, we simply cannot give a criminal a free pass. It is for that narrow set of circumstances that the FBI designed "Carnivore."

Carnivore is, in essence, a special filtering tool that can gather the information authorized by court order, and only that information. It permits law enforcement, for example, to gather only the email addresses of those persons with whom the drug dealer is communicating, without allowing any human being, either from law enforcement or the service provider, to view private information outside of the scope of the court's order. In other words, Carnivore is a *minimization* tool that permits law enforcement strictly to comply with court orders, strongly to protect privacy, and effectively to enforce the law to protect the public interest. In addition, Carnivore creates an audit trail that demonstrates exactly what it is capturing.

As with any other investigative tools, there are many mechanisms we have in place to prevent against possible misuse of Carnivore, and to remedy misuse that has occurred. The Fourth Amendment, of course, restricts what law enforcement can do with Carnivore, as do the statutory requirements of Title III and the Electronic Communications Privacy Act, and the courts.

For federal Title III applications, the Department of Justice imposes its own guidelines on top of the privacy protections provided by the Constitution, statutes and the courts. For example,

before Carnivore may be used to intercept wire or electronic communications, the requesting investigative agency must obtain approval for the Title III application from the Department of Justice. Specifically, the Office of Enforcement Operations (OEO) in the Criminal Division of the Department reviews each proposed Title III application to ensure that the interception satisfies the Fourth Amendment requirements, and is in compliance with applicable statutes and regulations. Even if the proposal clears the OEO, approval must be given by a Deputy Assistant Attorney General. Although this requirement of high-level review is required by Title III only with regard to proposed intercepts of wire and oral communications, the Department voluntarily imposes the same level of review for proposed interceptions of electronic communications (except digital-display pagers). Typically, investigative agencies such as the Federal Bureau of Investigation have similar internal requirements, separate and apart from Constitutional, statutory or Department of Justice requirements.

If the investigative agency and the Department of Justice approve a federal Title III request, it still must, of course, be approved by the proper court. The court will evaluate the application under the Fourth Amendment and using the familiar standards of Title III. By statute, for example, the application to the court must show, through sworn affidavit, why the intercept is necessary as opposed to other less-intrusive investigative techniques. The application must also provide additional detail, including whether there have been previous interceptions of communications of the target, the identity of the target (if known), the nature and location of the communications facilities, and a description of the type of communications sought and the offenses to which the communications relate. By statute and internal Department regulation, the interception may last no longer than 30 days without an extension by the court.

Courts also often impose their own requirements. For example, many federal courts require that the investigators provide periodic reports setting forth information such as the number of communications intercepted, steps taken to minimize irrelevant traffic, and whether the interceptions have been fruitful. The court may, of course terminate the interception at any time.

The remedies for violating Title III or ECPA by improperly intercepting electronic communications can include criminal sanctions, civil suit, and for law enforcement agents, adverse employment action. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

Carnivore itself also contains self-regulating features. For example, because of its sophisticated passive filtering features, it automates the process of minimization without intrusive monitoring by investigators, and simply disregards packets of information that do not satisfy the criteria in the court's authorization. Indeed, one of the most powerful privacy-protecting features of Carnivore is its ability to ignore information that is outside the scope of the court-ordered authority. For later verification, it also logs the filter settings. In addition, as a practical matter, Carnivore is not deployed except with close cooperation with the appropriate system provider. In any event, the FBI does not use Carnivore in every instance in which the court orders a Title III electronic communication intercept. Indeed, I understand that the Bureau uses Carnivore only in those instances when the service provider is unable to comply with the court order using its own equipment, or when the provider asks the FBI to use Bureau equipment.

As I testified in April, we face three major categories of challenges in trying to keep the Internet a safe and secure place for our citizens. These are:

1. Technical challenges that hamper law enforcement's ability to locate and prosecute criminals that operate online;
2. Certain substantive and procedural laws that have not kept pace with the changing technology, creating significant legal challenges to effective investigation and prosecution of crime in cyberspace; and
3. Resource needs that must be addressed to ensure that law enforcement can keep pace with changing technology and has the ability to hire and train people to fight cybercrime.

Carnivore is an investigative tool that assists us in meeting the first challenge. As we have witnessed, tracking a criminal online is not always an impossible task using our investigative tools. For example, last year federal and state law enforcement combined to successfully apprehend the creator of the Melissa virus and the individual who created a fraudulent Bloomberg News Service website in order to artificially drive up the stock price of PairGain, a telecommunications company based in California. Although we are proud of these important successes, we still face significant challenges as online criminals become more and more sophisticated.

In nearly every online case, tracking the online criminal requires law enforcement to attempt to trace the "electronic trail" from the victim back to the perpetrator. In effect, this "electronic trail" is the fingerprint of the twenty-first century -- only much harder to find and not as permanent as its more traditional predecessor. In the physical world, a criminal and his victim are generally in the same location. But cybercriminals do not have to physically visit the crime scene. Instead they cloak their illegal activity by weaving communications through a series of

anonymous remailers, by creating forged e-mail headers with powerful point and click tools readily downloadable from hacker websites, by using a "free-trial" account or two, or by "wiping clean" the logging records that would be evidence of their activity.

In some cases, the criminal may not even be in the same country as the victim. The global nature of the Internet, while one of the greatest assets of the Internet to law-abiding citizens, allows criminals to conduct their illegal activity from across the globe. In these cases, the need to respond quickly and track the criminal is increasingly complicated and often frustrated by the fact that the activity takes place throughout different countries. With more than 190 countries connected to the Internet, it is easy to understand the coordination challenges that face law enforcement. Furthermore, in these cases, time is of the essence and the victim may not even realize they have been victimized until the criminal has long since signed-off. Clearly, the technical challenges for law enforcement are real and profound.

This fact was made clear in the findings and conclusions reached in the recently released report of the President's Working Group on Unlawful Conduct on the Internet, entitled, "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet." This extensive report highlights in detail the significant challenges facing law enforcement in cyberspace. As the report states, the needs and challenges confronting law enforcement, "are neither trivial nor theoretical." The Report outlines a three-pronged approach for responding to unlawful activity on the Internet:

- I. Conduct on the Internet should be treated in the same manner as similar conduct offline, in a technology neutral manner.

2. We must recognize that the needs and challenges of law enforcement posed by the Internet are substantial, including our need for resources, up-to date investigative tools and enhanced multi-jurisdictional cooperation.
3. Finally, we need to foster continued support for private sector leadership in developing tools and methods to help Internet users to prevent and minimize the risks of unlawful conduct online.

I would encourage anyone with an interest in this important topic to review carefully the report of the Working Group. The report can be found on the Internet by visiting the website of the Department of Justice's Computer Crime and Intellectual Property Section, located at www.cybercrime.gov. In addition to the report, www.cybercrime.gov also contains other useful information on a wide array of Internet related issues, including the topic of today's hearing – privacy.

Despite the type of difficulties outlined in the Unlawful Conduct Report and discussed today, the Justice Department and law enforcement across this nation are committed to continuing to work together and with their counterparts in other countries to develop and implement investigative strategies to successfully track, apprehend, and prosecute individuals who conduct criminal activity on the Internet. In so doing, the same privacy standards that apply in the physical world remain effective online.

Mr. Chairman, the Department of Justice has taken a proactive leadership role in making cyberspace safer for all Americans. The cornerstone of our cybercrime prosecutor program is the Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS. CCIPS was founded in 1991 as the Computer Crime Unit, and became a Section in 1996. CCIPS

has grown from five attorneys in 1996 to nineteen today, and we need more to keep pace with the demand for their expertise. The attorneys in CCIPS work closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators," or CTC's, in U.S. Attorney's Offices around the nation. Each CTC receives special training and equipment and serves as the district's expert on computer crime cases. CCIPS and the CTC's work together in prosecuting cases, spearheading training for local, state and federal law enforcement, working with international counterparts to address difficult international challenges, and providing legal and technical instruction to assist in the protection of this nation's critical infrastructures. We are very proud of the work these people do and we will continue to work diligently to help stop criminals from victimizing people online.

I also note that public education is an important component of the Attorney General's strategy on combating computer crime. As she often notes, the same children who recognize that it is wrong to steal a neighbor's mail or shoplift do not seem to understand that it is equally wrong to steal a neighbor's e-mail or copy a proprietary software or music file without paying for it. To remedy this problem, the Department of Justice, together with the Information Technology Association of America (ITAA), has embarked upon a national campaign to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens. The "Cybercitizen Awareness Program" seeks to engage children, young adults, and others on the basics of critical information protection and security and on the limits of acceptable online behavior. The objectives of the program are to give children an understanding of cyberspace benefits and responsibilities, an awareness of consequences resulting from the misuse of the

medium and an understanding of the personal dangers that exist on the Internet and techniques to avoid being harmed.

Finally, Mr. Chairman, the Subcommittee may be aware that the Administration will soon be transmitting to Congress a legislative proposal addressing various issues relating to cyber-security. I know that the focus of today's hearing is the Carnivore program, and this is not the time to undertake any detailed discussion of the Administration's proposal. I would, however, like to mention two points that relate directly to today's discussion. First, the Administration supports raising the statutory standards for intercepting the content of electronic communications so they are the same as those for intercepting telephone calls: high-level approval, use only in cases involving certain predicate offenses that are specified by statute, and statutory suppression of evidence derived from improper intercepts. Second, the Administration supports requiring federal judges to confirm that the appropriate statutory predicates have been satisfied before issuing a pen register or trap-and-trace order. Those changes would apply to the use of Carnivore – and would, in important respects, simply confirm by statute the policies and procedures already followed by the Department of Justice. Beyond those specific points, I will simply note here that the Administration supports a balanced updating of laws to enhance protection of both privacy and public safety, and that the forthcoming proposal will contain important provisions whose enactment would be most helpful in the ongoing fight against cyber-crime.

Conclusion:

Mr. Chairman, I want to thank you again for this opportunity to testify today about our efforts to fight crime on the Internet while preserving the rights conferred by the Fourth Amendment and statute. Ultimately, the decision as to the appropriate parameters of law

enforcement activity lies squarely within the Constitution and the elected representatives of the people, the Congress. The need to protect the privacy of the American people, not just from the government but also from criminals, is a paramount consideration, not just in the context of the Internet, but in general. The Department of Justice stands ready to work with this Subcommittee and others to achieve the proper balance between the important need for protecting privacy and the need to respond to the growing threat of crime in cyberspace.

Mr. Chairman, that concludes my prepared statement. I would be pleased to attempt to answer any questions that you may have at this time.

ORAL STATEMENT OF KEVIN DI GREGORY

Mr. Chairman, and Members of the Subcommittee, thank you for allowing me this opportunity to testify about the law enforcement tool "Carnivore" and the Fourth Amendment.

We have seen magnificent growth of the Internet over the last ten years. It has created vast benefits for citizens, businesses and governments, and seems to hold boundless promise if we can harness it. The Internet has spurred a new and thriving economy. Many businesses have prospered by providing their products and services through the Internet. Others have assisted in building, maintaining and improving the Internet itself. The Internet has given people jobs, supported families and communities and created new opportunities for commerce for America and the world. The Internet has touched both our working lives and our family lives.

As we have seen throughout history, however, there are those who use the powerful tools of progress to inflict harm on others. The Internet has not escaped this historical truth. Even in the Internet's relatively short existence we have seen a wide range of criminal use of the technology. It has been used to commit traditional crimes against an ever widening number of victims. There are also those criminals intent on attacking and disrupting computers, computer networks and the Internet itself. In short, although the Internet provides an unparalleled opportunities for Americans to freely express ideas, it also provides a very effective means for ill-motivated persons to breach the privacy and security of others.

Many of the crimes that we confront everyday in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft, and child pornography are migrating to the Internet. The Fourth Amendment and laws addressing privacy and public safety serve as a framework for law enforcement to respond to this new forum for

criminal activity. If law enforcement fails properly to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cybercrime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is the key.

Despite the fervor over the unfortunately-named "Carnivore," the truth of the matter is that Carnivore is in reality a tool that helps us achieve this balance. To satisfy our obligations to the public to enforce the laws and preserve public safety, we use the same sorts of investigatory techniques and methods online as we do in the physical world, with the same careful attention to the strict constitutional and legal limits. Carnivore is simply an investigatory tool that helps us to investigate online in the same way as in the physical world, and enables us to obtain only the information we are authorized to obtain through a court order.

To illustrate, law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products, or to whom the drug dealer is selling his goods. It is therefore important to determine with whom the drug dealer is communicating. In the "olden days" of perhaps 10 years ago, the drug dealer would have communicated with his supplier and customers exclusively through use of telephones and pagers. Law enforcement would obtain an order from a court authorizing the installation of a "trap and trace" and a "pen register" device on the drug dealer's phone or pager. Now, that same drug dealer, or a kidnapper or a child

pornographer, may be just as likely to send an e-mail as to call his confederates.

When law enforcement uses a "trap and trace" or "pen register" in the online context, however, we have found that, at times, the Internet service provider has been unable or even unwilling to supply this information. It is for that narrow set of circumstances that the FBI designed "Carnivore." Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet. We cannot do this without tools like Carnivore.

Carnivore is, in essence, a special filtering tool that can gather the information authorized by court order, and only that information. It permits law enforcement, for example, to gather pursuant to an order only the email addresses of those persons with whom the drug dealer is communicating, without allowing any human being, either from law enforcement or the service provider, to view private information outside of the scope of the court's order. In other words, Carnivore is a minimization tool that permits law enforcement to comply with court orders, to protect privacy, and to enforce the law to protect the public interest. In addition, Carnivore creates an audit trail that demonstrates exactly what it is capturing.

And as with any other investigative tools, there are many mechanisms we have in place to prevent possible misuse of Carnivore, and to remedy misuse that has occurred. The Fourth Amendment and the courts, of course, restricts what law enforcement can do on line, with or without Carnivore, as do the statutory requirements of Title III and the Electronic Communications Privacy Act.

In the case of federal Title III applications, the Department of Justice imposes its own

guidelines on top of the privacy protections provided by the Constitution, statutes and the courts. For example, before Carnivore may be used to intercept wire or electronic communications, with the limited exception of digital display pagers, the requesting investigatory agency must obtain approval for the Title III application from the Department of Justice. Specifically, the Office of Enforcement Operations in the Criminal Division of the Department reviews each proposed Title III application to ensure that the interception satisfies the Fourth Amendment requirements, and is in compliance with applicable statutes and regulations. If the proposal clears the OEO, approval must generally be given by a Deputy Assistant Attorney General. Typically, investigative agencies such as the Federal Bureau of Investigation have similar but separate internal requirements.

If the investigative agency and the Department of Justice approve a federal Title III request, it still must, of course, be approved by the proper court using familiar but exacting standards. By statute and internal Department regulation, the interception may last no longer than 30 days without an extension by the court. And courts also often impose their own additional requirements.

In addition, the remedies for violating Title III or ECPA by improperly intercepting electronic communications include criminal sanctions and civil suits. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

Despite this panoply of protections, we recognize that concerns remain about this tool. Therefore, the Attorney General has asked for an independent review of the Carnivore source code to ensure that its capabilities are what we understand them to be. A report generated from the review will be publicly disseminated to interested groups within industry, academia and elsewhere, and should alleviate any concerns regarding unjustified intrusions on privacy from the

use of this tool.

Conclusion

Mr. Chairman, my testimony today necessarily highlights a few of the more significant aspects of the balance between privacy and security. The Department of Justice has provided the Committee with my full written statement. It is my sincere hope and expectation that through this and other fora, those of us who are concerned about privacy and public safety will recognize that responsible law enforcement can enhance both goals.

Wiretapping in Cyberspace

Millions of Americans now log on to the Internet as naturally and as frequently as they pick up a phone. Technology has created a revolution in personal communications, but technology is also making it possible for government and even employers to monitor private conversations as never before. Telephone-era laws must be updated to address these new challenges to privacy.

Last week the White House proposed some limited changes to the federal wiretap and electronic privacy laws that would raise legal standards for government interception of e-mail. Separately, several lawmakers introduced legislation to require employers to notify employees about how e-mail, Internet use and phone calls are monitored. Employees of The New York Times Company are already notified that the company reserves the right to review e-mail messages while investigating a complaint. Last year the company dismissed 23 employees — most based at a regional business office — for sending offensive e-mail messages.

In the absence of more stringent controls, law enforcement agencies may be tempted to conduct wholesale monitoring of digital written communications. It is probably not practical for agents to listen in on all the phone calls, for example, that go through AT&T. But new technology is making it possible for agencies like the F.B.I. to scan, read and record millions of pieces of e-mail on the network of an Internet service provider. Until now, this kind of power and its potential for abuse were not so readily available.

Current wiretapping laws were not drafted with this technology in mind and need to be updated. Various statutes now set different legal standards for the secret interception of domestic communications by law enforcement agencies, depending on whether the communication is by telephone, e-mail or cable modem.

The Clinton administration is proposing to

eliminate these inconsistencies. Its plan would bring the standards used for intercepting e-mail messages up to the stricter, more protective level now applied to telephone wiretaps. Illegal interception of e-mail would result in suppression of the evidence, as is the case now with illegal interception of phone calls. The proposal would also enforce the same legal standards that apply to phone calls for interception of e-mails sent by cable modems, which have a greater degree of privacy protection under a law that governs cable systems.

The administration is also calling for greater authority for courts to review law enforcement requests to use devices that record the phone numbers of incoming and outgoing calls and to track the origins and destinations of e-mail messages.

These changes are clearly needed. But Congress also needs to provide new safeguards against the government's wrongful use of ever more powerful surveillance technology against law-abiding citizens. Serious concerns have been raised about Carnivore, the new online wiretap system used by the F.B.I. to track the communications of individuals suspected of criminal activity.

The F.B.I. says the technology can isolate the e-mail of the target of an investigation. But the system, when hooked up to the network of the Internet service provider, gives the F.B.I. unlimited access to the e-mail of all other subscribers on the network. While a court order is still required to intercept the content of messages, the secret technology controlled exclusively by law enforcement raises fears of improper monitoring.

Until now, routine government surveillance of private conversations was limited as much by practicality as by legal constraints. Now that it is feasible to eavesdrop electronically on an unlimited scale, the laws have to be strengthened to prevent monitoring of all online communications simply because technology makes it easy.

The warning from Colombia's Serrano

Since the United States approved \$1.3 billion in counternarcotics aid for Colombia, guerrilla groups who profit from the drug trade have waged a bloody terror campaign in protest. Even as Colombian government officials and guerrilla leaders sat around a peace table in Geneva on Monday and Tuesday, the bloodshed in Colombia continued unabated.

Since January, when aid to Colombia was approved, the Revolutionary Armed Forces of Colombia (FARC), a guerrilla group, has attacked almost 200 police stations and killed more than 100 police officers. Fighting that began over the weekend in Colombia's northern San Lucas mountains appears to have resulted in the deaths of 60 members of the National Liberation Army (ELN) guerrilla group and 18 renegade, paramilitary fighters. In addition, on Monday 200 FARC terrorists ambushed a police station in the remote southwestern province of Narino, which is rich in opium poppy fields. The FARC gunned down 11 police officers and wounded 17 others.

This summit's context of violence highlights how brutal guerrilla and paramilitary tactics continue to be. Commanders for the FARC, which has effective control of about 40 percent of the country, declined even to attend the summit. But the relatives of 11 people kidnapped by the ELN in the spring of 1999 were there, lobbying for the release of their loved ones. The ELN's chief, Antonio Garcia, gave them little hope, pre-empting the summit by saying that neither the issue of hostages nor a cease-fire would be on the table for discussion.

What the ELN did want to discuss is the 1,500 square-mile territory that Colombian President Andres Pastrana has tentatively agreed to surrender to ELN control. But the agreement is difficult to implement since the area, which is rich in oil, gold and cocaine, is overrun by paramilitary forces.

In addition, local residents are strongly opposed to forfeiting the region to the ELN, since they fear living outside of the government's protection. The government gave the FARC control of a demilitarized zone about one year ago and an ombudsman appointed by Congress has documented 41 disappearances in the territory at the hands of the FARC. The territory was ceded as a land for peace deal, but the FARC now uses the demilitarized zone as a base of illegal operations and has shown no will whatsoever to negotiate a peace.

Former Colombian Police Chief Jose Serrano, who was in Washington last week to receive the DEA's special agent award, described the growing link guerrilla and paramilitary groups have formed with drug traffickers, giving terrorists access to vast resources to buy guns. "After the iron curtain fell, and subversives stopped receiving money from the former Soviet Union or Cuba, the FARC began attacking us when we fumigated [coca] crops," Mr. Serrano told The Washington Times. Mr. Pastrana's plan to achieve peace through counternarcotics initiatives and social projects is therefore "the last chance that we Colombians have. Because if it fails, we will have to make our peace over corpses," he said. No one should want that. Colombia has seen enough suffering.

Los Angeles Times

DATE: 7-27-00
PAGE: A-15

Who Needs Big Brother When There's 'Carnivore'?

■ **Law enforcement:** The FBI should not be granted such sweeping powers to search our e-mail and then be trusted to police itself.

By BART KOSKO

Now the FBI wants to recruit Internet service providers, or ISPs, to spy on U.S. citizens. The FBI already works with the credit companies to secretly snoop on large portions of our digital credit reports per the 1996 Intelligence Authorization Act. The FBI has installed digital phone-tapping equipment directly in phone companies under a similar congressional act passed in 1994. And the Treasury Department's Financial Crimes Enforcement Network has "deputized" all banks to monitor our bank accounts and to secretly file "suspicious activity reports" that it shares with the FBI and IRS and even with some foreign governments.

The FBI calls its new ISP surveillance software "Carnivore." An agent connects a laptop to the ISP server and then reads at least the address of every e-mail message that passes through the server. The FBI says it has used its Carnivore software 25 times in the last two years to search for terrorists or drug dealers or child pornographers. The FBI claims that it needs this search-e-mail software to help it find and catch such criminals when they use the Internet.

There are three problems with Carnivore, and each is fatal. The first is that Carnivore undermines the 4th Amendment's ban on unreasonable searches—if it does not violate it outright. The FBI still must get a judge to issue a search warrant based on "probable cause." This in practice can mean no more than that the FBI asks for the warrant. But the 4th Amendment further demands that the warrant be specific—"particularly describing the place to be searched."

Carnivore searches blindly through all private e-mails that flow through the ISP server while it looks for a suspicious few. This is as if the police have a warrant to search someone's bedroom closet and then search all houses in a city until they find it. The search itself invades privacy.

Carnivore switches the order of search and identification. Traditional searches first identify the suspect's property, which is then searched. Carnivore searches through private databases until it identifies a suspect's property—and

perhaps learns some new things along the way. This is a big leap down the slippery slope of state invasion of privacy. And the very existence of such a monitoring system produces a chilling effect on e-mail-based free speech, because knowing that a state police agency will read at least part of your e-mail message affects what you say in that message.

The second problem is that the FBI does not need Carnivore to search for alleged criminal e-mails. Rep. John Conyers Jr. (D-Mich.) raised this issue with FBI Assistant Director Donald Kerr when Kerr testified before Congress at a hearing Monday on Carnivore: "Why do we need to put terminals on site at the ISPs rather than let the ISP itself turn over needed information much in the way that telephone companies do?"

Kerr conceded this point but claimed that the FBI still needs Carnivore for those ISPs that lack filtering software. This is plainly specious: The FBI or oversight sources could simply give such ISPs this filtering software. There is simply no need to grant the FBI such sweeping powers of search and then trust the agency to police itself as those powers inevitably grow in time.

The third problem is that Carnivore ultimately will not work despite all its costs. The criminals it tries to watch are the very people who will take the two obvious steps to evade it: They will change their fake digital IDs more often, and they will use ever more powerful digital encryption to scramble their messages.

Carnivore's software blueprints and performance quirks themselves will leak to the digital underground despite or because of the best efforts of those in Congress or the judiciary who oversee it. And hackers will surely study the software system and maybe crack it.

The only people Carnivore can confidently watch are the innocent citizens whom it has no right to watch. This sets a foolish and dangerous precedent for the type of heavy-handed government surveillance one would expect to find in Myanmar or China.

The only thing right about Carnivore is its name: This digital beast devours both personal privacy and constitutional limits on state police power. Congress should kill it.

Bart Kosko is a professor of electrical engineering at USC and the author of "The Fuzzy Future" (Random House, 1999).

18

Microsoft Files Brief Asking Supreme Court to Send Antitrust Case to Appeals Court

By STEVE LOHR

In a legal document filed yesterday, Microsoft argued that the government's antitrust case is "completely unsuitable for direct appeal" to the Supreme Court because it is complex and because the trial judge made "serious and substantive procedural errors."

Microsoft wants its appeal to go first to the federal appeals court in Washington, which ruled in favor of the company in a related case.

The company's argument, filed with the Supreme Court, rests heavily on a scathing attack on the work of Judge Thomas Penfield Jackson, who heard the lawsuit in Federal District Court.

The Microsoft document, citing interviews Judge Jackson granted to new organizations, including The

New York Times, stated, "The district court's blunt comments to the press raise serious questions about its impartiality."

Microsoft also questioned the even-handedness of Judge Jackson's decisions in general. First, the company asserted, the judge improperly allowed the Justice Department and 19 states suing the company to broaden their case. Then, after allowing the additional evidence, Judge Jackson assured the company that his findings would be based on the more limited, original complaint, according to the Microsoft filing.

Those "assurances," the company stated, "the district court would later repudiate."

Judge Jackson ruled earlier this year that Microsoft was a monopolist that had repeatedly violated antitrust laws, and he ordered that the company be split in two — an order he later shelved pending appeals.

If the case goes straight to the Supreme Court, it could be resolved in a year. If it goes first to the appeals court, the resolution might take up to two years.

The government is seeking to have the Supreme Court hear the appeal directly and sidestep a review by a federal appeals court. Direct appeals to the court are permitted in major antitrust cases brought by the government. Four of the nine justices must vote in favor for the case

to go directly from the district court.

In its filing, Microsoft is trying to persuade the court that the appeal will involve a thicket of technical issues, procedural challenges and disputed facts. Sorting out these matters, Microsoft says, will involve poring over the voluminous written record of the lengthy trial — precisely the kind of winnowing usually left to an appeals court. The Justice Department had no comment yesterday,

The software company says the trial judge made procedural errors.

other than a brief statement saying that the government "will respond in its filing."

Still, there is little mystery about what the government's theme will probably be when it files its brief with the court on Aug. 15. First, according to legal experts, the government will say that the factual findings are clear and that the issues for appeal are a couple of big legal questions — precisely the kind of major judgments of law that the court so often reserves for itself.

The big legal issues, they say, are whether Microsoft's bundling of its Internet browser with its industry-standard Windows operating system was an illegal tying of two products and whether Microsoft's dealings with other companies was indeed "monopolizing conduct," in legal parlance. Judge Jackson ruled that Microsoft's bundling move and its behavior did violate antitrust laws, and Microsoft is appealing his ruling.

The government is also expected to make a forceful policy argument for the expedited appeal, given the importance of computer industry to the economy.

"The government will say that Microsoft's monopoly is imposing a significant social cost while this case is on appeal and no remedies are in place," said Herbert Hovenkamp, a professor at the University of Iowa law school. "It will say that not taking the case is a costly act, and that this is exactly the kind of case that

was meant to go directly to the Supreme Court."

In its 30-page filing, Microsoft stated that the case "went badly awry from the outset," referring to Judge Jackson's decision to permit the government to add additional evidence after the suit was filed in May 1998.

That move, Microsoft said, allowed the Justice Department and states to "transform their case beyond recognition." In doing so, Microsoft declared that the judge "committed an array of serious and substantive procedural errors."

These errors, Microsoft said, included giving the company too little time for discovery and preparation of its defense to the expanding array of evidence.

Much of the evidence in the case, Microsoft contends, should have been tossed aside as not being suitable for admission in court. "The district court," Microsoft stated, "largely suspended application of the federal rules of evidence, admitting numerous newspaper and magazine articles and other rank hearsay."

Judge Jackson, legal analysts say, did allow a wide range of written evidence in the case. But he gave that leeway to both sides, they said, noting that Microsoft submitted many newspaper articles, even press releases, as evidence.

And the government maintained that the additional evidence presented after the complaint was filed was part of the "pattern" of anti-competitive practices Microsoft used to stifle competition. Thus, the government said, the additional evidence involving companies like Intel and Apple was not an expansion of the original complaint, but merely further examples that fit the same pattern of behavior. Judge Jackson agreed with the government.

In its filing, Microsoft suggested that in its appeal, the company will seek to make sure that it no longer appears before Judge Jackson. It said his comments to the press should be considered grounds for a

ADDITIONAL CARNIVORE DOCUMENTS

FROM

**OFFICE OF GENERAL COUNSEL
TECHNOLOGY LAW UNIT
(THROUGH 7/28/00)**

PAGES REVIEWED: 49

PAGES RELEASED: 49

**EXEMPTIONS CITED: b6-1, b7C-1,
b6-3 & b7C-3**

**NOTE: 91 pages from this file are duplicates to pages from
The Office of General Counsel's Front Office file.**



In-Congress

**American Civil Liberties Union
Freedom Network**

July 11, 2000

VIA FAX

Hon. Charles T. Canady, Chairman
Constitution Subcommittee of the
House Judiciary Committee
362 Ford House Office Bldg.
Washington, D.C. 20515-6220

and

Hon. Melvin L. Watt, Ranking Member
Constitution Subcommittee of the
House Judiciary Committee
362 Ford House Office Bldg.
Washington, D.C. 20515-6220

Dear Representatives Canady and Watt:

We are writing to you about the new FBI email surveillance system aptly named "Carnivore," which gives law enforcement extraordinary power to intercept and analyze huge volumes of email. The Carnivore system gives law enforcement email interception capabilities that were never contemplated when Congress passed the Electronic Communications Privacy Act (ECPA), codified in relevant part at 18 U.S.C. 2510-22 and 18 USC 3121-27. Carnivore raises new legal issues that cry out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age.

The existence of Carnivore first came to light in the April 6 testimony of Attorney Robert Corn-Revere to the Constitution Subcommittee. Its operation was further detailed in a report that appeared in today's Wall Street Journal (copy attached). According to these reports, the Carnivore system -- essentially a computer running specialized software-- is attached directly to an Internet Service Provider's (ISP) network. Carnivore is attached either when law enforcement has a Title III order from a court permitting it to intercept in real time the contents of the electronic communications of a specific individual, or a trap and trace or pen register order allowing to it obtain the "numbers" related to communications from or to a specified target.

But unlike the operation of a traditional a pen register, trap and trace device, or wiretap of a conventional phone line, Carnivore gives the FBI access to all traffic over the ISP's network, not just the communications to or from a particular target. Carnivore, which is capable of analyzing millions of messages per second, purportedly retains only the messages of the specified target, although this process takes place without scrutiny of either the ISP or a court.

Carnivore permits access to the email of every customer of an ISP and the email of every person who communicates with them. Carnivore is roughly equivalent to a wiretap capable of

accessing the contents of the conversations of all of the phone company's customers, with the "assurance" that the FBI will record only conversations of the specified target. This "trust us, we are the Government" approach is the antithesis of the procedures required under our the wiretapping laws. They authorize limited electronic surveillance of the communications of specified persons, usually conducted by means of specified communications devices. They place on the provider of the communications medium the responsibility to separate the communications of persons authorized to be intercepted from other communications.

Currently, law enforcement is required to "minimize" its interception of non-incriminating communications of a target of a wiretap order. Carnivore is not a minimization tool. Instead, Carnivore maximizes law enforcement access to the communications of non-targets.

In his testimony to your subcommittee Mr. Corn-Revere described the experience of his client, an ISP that was required to install Carnivore when presented with a trap and trace order. He detailed his client's concerns that a trap and trace order in the context of the Internet revealed information that Congress did not contemplate when it authorized their limited use. In the traditional telephone context, those orders reveal nothing more than the numbers dialed to or from a single telephone line. In the Internet context, these orders and certainly Carnivore, likely involve ascertaining the suspect's e-mail address, as well as header information that may provide information regarding the content of the communication.

As we have stated previously, the ACLU does not believe that it is clear that the Government can serve an order on an Internet service provider and obtain the e-mail addresses of incoming and outgoing messages for a particular subscriber. Further, it is not clear whether law enforcement agents use or should use authority under the pen register statute to access a variety of data, including Internet Protocol addresses, dialup numbers and e-mail logs. We certainly do not believe that it is clear that law enforcement can install a super trap and trace device that access to such information for all of an ISP's subscribers.

In light of the new revelations about Carnivore, the ACLU urges the Subcommittee to accelerate its consideration of the application of the 4th Amendment in the digital age. Legislation should make it clear that law enforcement agents may not use devices that allow access to electronic communications involving only persons other than a specified target for which it has a proper order. Such legislation should make clear that a trap and trace order served on an ISP does not authorize access to the contents of any communication - including the subject line of a communication -- and that the ISP bears the burden of protecting the privacy of communications to which FBI access has not been granted.

We would be happy to work with the Subcommittee on drafting legislation that protects the privacy rights of Americans.

Sincerely,

Laura W. Murphy
Director, ACLU Washington National Office

Barry Steinhardt
Associate Director, ACLU

Gregory T. Nojeim

Legislative Counsel, ACLU Washington National Office

cc: Members of the Constitution Subcommittee of the House Judiciary Committee

[\[Legislative Archives\]](#) [\[106th Congress Issues\]](#) [\[Voters' Guide\]](#) [\[Congress Overview\]](#) [\[How to Use this Section\]](#)

[INDEX](#)

[JOIN](#)

[HOME](#)

[SEARCH](#)

[FEEDBACK](#)

Copyright 1999, The American Civil Liberties Union

Want to send this story to another AOL member? Click on the heart at the top of this window.

Stronger Online Privacy Sought

By D. IAN HOPPER
c. The Associated Press

WASHINGTON (AP) - Lawmakers are seeking ways to shore up online privacy following reports of businesses selling customers' personal information and an FBI system that hunts for suspects by scanning citizens' e-mail.

Sens. Patrick Leahy, D-Vt., and Robert Torricelli, D-N.J., introduced legislation that would bar the sale of personal information kept by a defunct company if the sale would have violated privacy policies in effect when the company was in business.

The bill responds to the case of Toysmart, a former online toy retailer that put all its assets, including its customer records - such as names, addresses and credit card numbers - up for sale despite a privacy policy that assured customers the information would remain private.

The Federal Trade Commission filed a suit against Toysmart this week to stop the sale from taking place. Rep. Spencer Bachus, R-Ala., has already announced plans to introduce a similar bill in the House.

"It is wrong to use our nation's bankruptcy laws as an excuse to violate a customer's personal privacy," the senators said in a letter to colleagues asking for support for the bill. "Customers have a right to expect a firm to adhere to its privacy policies, whether it is making a profit or has filed for bankruptcy."

The legislators say they will try to include the bill in a larger bankruptcy reform package.

TRUSTe, an organization that gives its seal to Web sites that meet its privacy principles, blew the whistle on Toysmart in June.

Earlier Wednesday, Walt Disney, the majority owner of Toysmart, said it has offered to purchase the company's lists and assure their confidentiality.

In a related action, two legislators are going after "Carnivore," a system in use by the FBI to monitor suspected criminals' e-mail. Carnivore is installed at a suspect's Internet provider and scans through all incoming and outgoing mail, looking for messages belonging to the suspect.

Privacy groups, such as the American Civil Liberties Union and the Electronic Information Privacy Center, and some Internet providers object to the system because Internet companies have no control over the "black box." They say it infringes upon the rights of individuals not involved with the FBI investigation.

The ACLU sent a letter to Rep. Charles Canady, R-Fla., detailing its concerns. Canady will announce Thursday the date for hearings on Carnivore, his spokesman said.

House Majority Leader Dick Armey sent a letter Wednesday to Attorney General Janet Reno and FBI Director Louis Freeh blasting the agencies and the Clinton administration for the "cybersnooping" system.

"The federal government has the power and the authority to collect and maintain vast amounts of private personal information," wrote Armey, R-Texas. "This administration continues to demonstrate a cavalier attitude with that responsibility."

Also, Rep. Clay Shaw, R-Fla., will introduce a bill Thursday aimed at stopping identity theft. The bill would prohibit the sale of Social Security numbers, which can be used to get credit card numbers, bank loans and accounts in another person's name. The FTC announced Wednesday that calls to their identity theft hot line are on the rise, at about 850 reports per week.

"Identity theft is a terrible problem that has literally destroyed people's lives and it must be stopped," said Shaw, who heads the House Social Security subcommittee.

On the Net: TRUSTe: <http://www.truste.org>

American Civil Liberties Union: <http://www.aclu.org>

Privacy International: <http://www.privacy.org/pi/>

AP-NY-07-12-00 1915EDT

Copyright 2000 The Associated Press. The information contained in the AP news report may not be published, broadcast, rewritten or otherwise distributed without the prior written authority of The Associated Press. All active hyperlinks have been inserted by AOL.

FBI Cybersnooping System Raises Additional Privacy Concerns

Armey to Administration: Stay Out of My Inbox!
July 12, 2000



Related Links

[The e-Contract](#)

[Remarks on the e-Contract with High Tech America](#)

[FBI Cybersnooping System Raises Privacy Concerns](#)

[Only Violate Personal Privacy in the Right Way?](#)

[Is the Government in a Position to Talk About Internet Privacy?](#)

House Majority Leader Dick Armey today called on Attorney General Janet Reno and FBI Director Louis Freeh to address the privacy concerns raised by the Federal Bureau of Investigation's Carnivore system of monitoring email traffic. Armey issued the following statement:

This Administration doesn't have the best record on personal privacy. It keeps repeating the same mistake over and over.

Last year, a draft Administration proposal for a computer network monitoring system called FIDNet surfaced. When I joined privacy advocates in questioning the legitimacy of a government system that could monitor *private sector* networks, the Administration backed off a bit from their original design. But it has yet to answer my question of why they intended to monitor private systems in the first place.

Now the FBI wants to run a system that could sort through every single e-mail message that passes through a commercial Internet service provider. I ask, why should we trust this Administration with our most personal correspondence?

At a time when there is a lot of talk about concerns for Internet privacy, the Clinton-Gore Administration continues to push Big Brother proposals that promote government cybersnooping. They seem tone deaf to the concerns people have about the government invading their privacy. The Federal government has the power and the authority to collect and maintain vast amounts of private personal information. This Administration continues to demonstrate a cavalier attitude with that responsibility.

I call on Attorney General Reno and FBI Director Freeh to stop using this cybersnooping system until fourth amendment concerns are adequately addressed.

Related Correspondence:

- [First letter to AG Reno](#)
- [Second letter to AG Reno](#)
- [Third letter to AG Reno](#)
- [Privacy violations at ONDCP](#)
- [Letter to the president on web privacy](#)

- [Letter to the IRS on privacy violations](#)

get
e-mail
updates!

[Front Page](#) | [Get Updates](#) | [Features](#) | [News & Info](#) | [Search](#)
Freedom Works : Home Page of the Office of the House Majority Leader

freedom
works

CARNIVORE

Diagnostic Tool

The Nation's communications networks are routinely used in the commission of serious criminal activities, including espionage. Organized crime groups and drug trafficking organizations rely heavily upon telecommunications to plan and execute their criminal activities.

The ability of law enforcement agencies to conduct lawful electronic surveillance of the communications of its criminal subjects represents one of the most important capabilities for acquiring evidence to prevent serious criminal behavior. Unlike evidence that can be subject to being discredited or impeached through allegations of misunderstanding or bias, electronic surveillance evidence provides jurors an opportunity to determine factual issues based upon a defendant's own words.

Under Title III, applications for interception require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorneys offices can apply for such orders. Interception orders must be filed with federal district court judges or before other courts of competent jurisdiction. Hence, unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offense(s) being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses that are anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence -- not intelligence.

Applications must indicate that other normal investigative techniques will not work or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are limited to 30 days and interceptions must terminate sooner if the objectives are obtained. Judges may (and usually do) require periodic reports to the court (typically every 7-10 days) advising it of the progress of the interception effort. This circumstance thus assures close and ongoing oversight of the electronic surveillance by the United States Attorney's office handling the case. Extensions of the order (consistent with requirements of the initial application) are permitted, if justified, for up to a period of 30 days.

Electronic surveillance has been extremely effective in securing the conviction of more than 25,600 dangerous felons over the past 13 years. In many cases there is no substitute for electronic surveillance, as the evidence cannot be obtained through other traditional investigative techniques.

In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many Internet Service Providers (ISP) lacked the ability to discriminate communications to identify a particular subject's messages to the exclusion of all others, the FBI designed and developed a diagnostic tool, called Carnivore.

The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept. This type of tool is necessary to meet the stringent requirements of the federal wiretapping statutes.

The Carnivore device works much like commercial "sniffers" and other network diagnostic tools used by ISPs every day, except that it provides the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not. For example, if a court order provides for the lawful interception of one type of communication (e.g., e-mail), but excludes all other communications (e.g., online shopping) the Carnivore tool can be configured to intercept only those e-mails being

transmitted either to or from the named subject.

Carnivore serves to limit the messages viewable by human eyes to those which are strictly included within the court order. ISP knowledge and assistance, as directed by court order, is required to install the device.

The use of the Carnivore system by the FBI is subject to intense oversight from internal FBI controls, the U. S. Department of Justice (both at a Headquarters level and at a U.S. Attorney's Office level), and by the Court. There are significant penalties for misuse of the tool, including exclusion of evidence, as well as criminal and civil penalties. The system is not susceptible to abuse because it requires expertise to install and operate, and such operations are conducted, as required in the court orders, with close cooperation with the ISPs.

The FBI is sharing information regarding Carnivore with industry at this time to assist them in their efforts to develop open standards for complying with wiretap requirements. The FBI did so two weeks ago, at the request of the Communications Assistance for Law Enforcement Act (CALEA) Implementation Section, at an industry standards meeting (the Joint Experts Meeting) which was set up in response to an FCC suggestion to develop standards for Internet interception.

This is a matter of employing new technology to lawfully obtain important information while providing enhanced privacy protection.

| Programs and Initiatives | FBI Home Page |

66-1/67c-1

From: [REDACTED] 66-1/67c-1
 To: KERR, DONALD
 Date: Tuesday, July 18, 2000 9:24PM
 Subject: CARNIVORE BRIEFING FOR DAG 2PM 7/19

Dr. Kerr,

I received a call this evening from [REDACTED] relaying a request from the DAG's Office that you and [REDACTED] be available for a briefing of Deputy Attorney General Eric Holder tomorrow in Mr. Holder's Conference Room (room 4111) at DOJ at 2:00 PM. [REDACTED] requested my presence as well. [REDACTED] was previously scheduled to brief DOJ at 12:30. I have contacted him and he has confirmed that the briefing has been rescheduled for 2:00 PM and will now include the DAG. I will have to come back in from CART at Fredericksburg, or another representative of OGC will be present.

We have been asked to confirm our attendance by contacting [REDACTED] at [REDACTED]

Technology Law Unit
 Office of the General Counsel
 FEDERAL BUREAU OF INVESTIGATION
 935 Pennsylvania Ave., N.W. Rm [REDACTED]
 Washington, D.C. 20535-0001
 Tel [REDACTED]
 Fax [REDACTED]
 Pag [REDACTED]
 No Internet E-Mail Address

CC: [REDACTED]

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

- ☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☐ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☐ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.
- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of DOC #4, OGC FRONT OFFICE

_____ Page(s) withheld for the following reason(s):

DOCS., WALL STREET
JOURNAL ARTICLE (7/14/00)
(PAGE 4)

- ☒ The following number is to be used for reference regarding these pages:

DOCUMENT # 6 (Page 165)

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXX
XXXXXX

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

- ☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☐ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☐ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.
- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

14 Pages were not considered for release as they are duplicative of Doc #13 PGS 1-14 OGC FRONT
OFFICE FILE (PGS 20-33)

_____ Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

Doc #8 (Pages 167-180)

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXX
XXXXXX

From: [REDACTED]
To: CHARLES STEELE, [REDACTED]
Date: 7/21/00 5:48PM
Subject: Latest version

66-1
67C-1

Charlie [REDACTED]

Attached is a copy of the statement with the DOJ revisions having been made.

66-1 / 670-1

Statement for the Record of
Donald M. Kerr
Assistant Director
Federal Bureau of Investigation
Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.
7/24/2000

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the FBI's Internet and data interception capabilities and to help set the record straight regarding this important issue. I would like to first discuss the FBI's legal authority for conducting interceptions on the Internet, and then describe the technical means by which we intercept Internet communications in order to obtain evidence of Federal felonies.

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search E-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting a part of our interception software - codenamed Carnivore as an ominous new technology that raised concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that our statutory law enforcement authorities be discussed openly. In fact, this was the reason we chose to share information about this capability with industry experts several weeks ago. As technology continues its rapid evolution, it is essential for the public to know and understand their government is scrupulously observing the laws and the constitutional protections that guarantee their right to privacy. It is also very important that these discussions be placed into their proper context and that the relevant facts concerning this issue are made clear. I welcome this opportunity to stress that our capabilities are used only after lawful court ordered authorization and that they are directed at the most serious violations of national security and public safety.

66-1/670-1

The FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), which is commonly referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". All such interceptions, with the exception of a rarely used "emergency" authority or in cases involving the consent of a participant in the communication, are conducted pursuant to court orders. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated. Last year, the FBI obtained Title III court orders in 327 instances. We did not initiate surveillances under emergency provisions of Title III.

Federal surveillance laws supplement the Fourth Amendment's dictates concerning reasonable searches and seizures to oral, wire and electronic communications. They also include a number of additional provisions which ensure that this investigative technique is used judiciously, with deference to the privacy of intercepted subjects.

An application for a warrant to search a private residence must be presented under oath to a judge or magistrate who may issue the warrant only upon a finding of probable cause to believe that a crime has been committed, and that specified evidence of the crime will be found in the place to be searched. Applications for Title III interceptions of wire, oral or electronic communications must be presented to judges in the same way (magistrates are not authorized to approve Title III applications). However, before the application can even be submitted to the court, it must be authorized by a senior official of the Department of Justice (DOJ). Title III requires such high-level approval for applications to intercept oral and wire communications, except in the case of digital pagers, and DOJ policy requires the same level of approval for applications to intercept

66-1/670-1

electronic communications, even though the law would allow lower-level approval.

Applications for electronic surveillance describe with particularity and specificity the particular offenses being committed, the communications facility or place from which the subject's communications are to be intercepted, a description of the types of communications to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Under Title III, electronic surveillance for criminal investigations is permitted only for the purpose of gathering hard evidence-- not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are obtained. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United-States Attorney's office handling the case. Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects or others not named in the application.

To ensure the evidentiary integrity of intercepted communications they must be recorded, if possible, on magnetic tape or other devices, so as to protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings must be presented to the federal district court judge and sealed under his or her directions. The presence of the seal is a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

66-1 / 67C-1

Within a reasonable period of time after the termination of the interception order, the judge is obligated by law to ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory that includes notice of the order, the dates during which the interceptions were carried out, and whether or not the communications were intercepted. Upon motion, the judge may also direct that portions of the contents of the intercepted communication be made available to affected persons for their inspection.

A variety of sanctions are available to penalize interceptions conducted in violation of Title III, ECPA and the Fourth Amendment. The evidence obtained through such unlawful interceptions can be suppressed. The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, may recover in a civil action against the person or entity engaged in the violation, damages, including punitive damages, attorney's fees and other costs.

Once we obtain an order for surveillance of wire communications, we generally require technical assistance from the carrier or service provider. Such help is increasingly necessary the case with the advent of advanced communications services and networks such as the Internet. The days of connecting a pair of alligator clips connecting a tape recorder to a copper wire phone are long gone. Title III mandates service provider assistance incidental to law enforcement's execution of electronic surveillance orders. Upon the request of the applicant, a court order authorizing the interception of communications may direct that a telecommunications "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted."

66-1/670-1

In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are also subject to the electronic surveillance laws, meaning that unauthorized electronic surveillance of their customers (or anyone else) is forbidden, and criminal and civil liability may be assessed for violations. The prohibition on using or disclosing the contents of communications illegally intercepted, likewise extends to service providers and their personnel. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in most cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue orders for Title III interceptions more narrowly tailored than those in the early years of Title III existence that were directed against "plain old telephone services." To be successfully implemented, these orders require complex methods to ensure that only messages for which there is probable cause to intercept are, in fact, intercepted. The increased detail in court orders issued under Title III responds to two relatively recent developments.

First, the complexity of modern communications networks, such as the Internet, and the complexity of modern users' communications equipment require better discrimination than older analog communications. For example, Internet users frequently use electronic messaging services,

66-1 / 670-1

like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call. Similarly, some Internet services, like streaming video, have more in common with broadcast media like television, than with telephone calls. These types of communications are less commonly the targets of an interception order.

Second, for many Internet services, users share communications channels, addresses, etc. These factors make the interception of messages for which law enforcement has probable cause, to the exclusion of all others, very difficult. Court orders therefore increasingly include detailed instructions to preclude the interception of communications that lie outside the scope of the order.

In response to a critical need for tools to implement complex court orders, the FBI developed a number of capabilities including the software program that is known as "Carnivore." The committee may be aware that Internet transmissions are broken down into packets of information consisting of a string of words or symbols. Different packets from the same message often take different routes between the sender and the intended recipient. The various packets constituting a single message are labeled so that they can be reassembled and read by the recipient. The challenge for law enforcement implementing a court order for interception of E-mail is to find and retrieve only those packets that are part of a message covered by the order. To do this, we developed a software solution to perform network analysis. This software runs on a standard personal computer running the standard Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programed in conformity with the court order. This filter set can be extremely complex, but it provides the FBI with an ability to collect only those transmissions which comply with pen register court orders, trap & trace court orders, and Title III interception orders.

66-1/6709

It is important to understand what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what our software does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use this program at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how we use the system in practice. First, there is the issue of scale. Carnivore is a small-scale tool intended for use only when and where it is needed. In fact, each one is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.

The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is

66-1/67c-9

connected by a high impedance bridge and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that our system is satisfactorily isolated from the network to which it is attached. Also, it is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This leads to the third issue--that of ISP cooperation. To my knowledge, we have never installed this system onto an ISP's network without assistance from the ISP's technical personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, and I can assure you that without the technical knowledge of the ISP's personnel, it would be difficult, if not impossible, for law enforcement agencies to successfully implement and comply with the strict language of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using this system is data integrity. As you know, Rule 901 of the Federal Rules of Evidence requires the authentication of evidence as a condition of its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is another reason for preferring this system to commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices without lawful authorization from a court. Over the last five years or more, we have witnessed a continuing, steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities that have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively

66-1/67c

investigate and prevent these crimes is, in part, dependant upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so without the continued cooperation of our industry partners and innovations such as the Carnivore software.

I look forward to working with the subcommittee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank You.

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

- ☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☐ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☐ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

76 Pages were not considered for release as they are duplicative of DOCUMENT #14, OGC FRONT
OFFICE FILE
(PAGES 45-120)

Page(s) withheld for the following reason(s):

- ☒ The following number is to be used for reference regarding these pages:

DOCUMENT #10 (PAGES 191-266)

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXX
XXXXXX

CENTER FOR DEMOCRACY & TECHNOLOGY

[Our Mission](#) / [Get Involved](#) / [Staff](#) / [Publications](#) / [Links](#) / [Search CDT](#) / [Jobs](#) / [Action!](#)

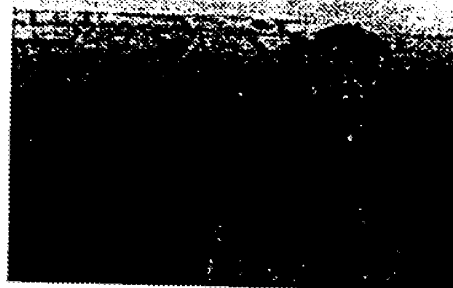
July 24, 2000

Alan Davidson

Staff Counsel

abd@cdt.org [Recent Presentations](#)

Alan Davidson is Staff Counsel at the Center for Democracy and Technology (CDT), a Washington D.C. non-profit group working to promote civil liberties on the Internet and other new digital media. Mr. Davidson is currently leading CDT's efforts to promote encryption policies that protect privacy and free expression in the information infrastructure. He has written and spoken widely on the civil liberties implications of public policies that restrict encryption, and has been directly involved in the ongoing Congressional debate over cryptography legislation.



Mr. Davidson also works more broadly on issues relating to Internet policy including free speech and censorship, Internet governance, digital signatures and electronic commerce, domain name issues, and online gaming. He took part in CDT's coordination of one of the two victorious challenges to the Communications Decency Act at the Supreme Court in *ACLU v. Reno*. His other research interests lie generally in the areas of privacy, free speech, and the special problems posed by the interaction of technology, public policy, and the law.

Mr. Davidson was a computer scientist before joining the legal profession. His earliest hacker credentials came as the proud owner of a Commodore PET in the late 1970s. A graduate of the Massachusetts Institute of Technology, he received an S.B. in Mathematics and Computer Science and later returned for an S.M. in Technology and Policy. Mr. Davidson worked as a Senior Consultant at Booz-Allen & Hamilton, designing the information systems for NASA's Space Station Freedom Project. He has also worked on technology and policy issues at the U.S. Congress Office of Technology Assessment and for the White House Office of Policy Development Health Care Task Force.

Mr. Davidson attended law school at Yale, where he was Symposium Editor of the Yale Law Journal. He remains active in MIT alumni affairs, and recently completed a 4-year term as a Trustee of the MIT Corporation. He also enjoys backpacking, skiing, and is currently learning to speak Spanish.

[Previous Headlines](#) | [Action](#) | [Legislative Tracking](#) | [CDT's Privacy Policy](#)
[Free Speech](#) | [Data Privacy](#) | [Wiretapping](#) | [Cryptography](#) | [Domain Names](#) | [International](#) | [Bandwidth](#) | [Security](#) | [Terrorism](#) | [Authentication](#) | [Right to Know](#)

[Our Mission](#) / [Get Involved](#) / [Staff](#) / [Publications](#) / [Links](#) / [Search CDT](#) / [Jobs](#) / [Action!](#)

©2000 The Center For Democracy & Technology
1634 Eye Street NW, Suite 1100
Washington, DC 20006
(v) 202.637.9800
(f) 202.637.0968

Technical concerns about this site: webmaster@cdt.org
Concerns or opinions about issues: feedback@cdt.org



American Civil Liberties Union
Freedom Network

In Unique Tactic, ACLU Seeks FBI Computer Code On "Carnivore" and Other Cybersnoop Programs

FOR IMMEDIATE RELEASE
Friday, July 14, 2000

WASHINGTON -- In what may be the first request of its kind, the American Civil Liberties Union is asking the Federal Bureau of Investigation to disclose the computer source code and other technical details about its new Internet wiretapping programs.

In a Freedom of Information Act (FOIA) request sent today to the FBI, the ACLU is seeking all agency records related to the government e-mail "cybersnoop" programs dubbed Carnivore, Omnivore and Etherpeek, including "letters, correspondence, tape recordings, notes, data, memoranda, email, computer source and object code, technical manuals, [and] technical specifications."

Computer "source code" is the set of instructions for a program written by its creators, which is compiled into "object code" which can be read by machines.

"Right now, the FBI is running this software out of a black box," said Barry Steinhardt, Associate Director of the ACLU and author of the letter. "The FBI is saying, 'trust us, we're not violating anybody's privacy.' With all due respect, we'd like to determine that for ourselves."

To the ACLU's knowledge, the request for program source code is the first of its kind. But Steinhardt said that two federal appeals court rulings that computer code is a form of speech, no different from any other written document, support the ACLU's demand under the the Freedom of Information Act. The Act gives Americans broad rights to obtain written information held by the federal government.

Technical data on traditional telephone wiretaps is currently available in public documents, Steinhardt said. Similar access to the computer source code of Carnivore and other such programs is necessary to determine just how the software operates and whether e-mail privacy is being violated.

The unbridled uses of these technologies "cry out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age," the ACLU said in a July 11 letter to members of Congress.

Revelations about the Carnivore program also prompted calls for disclosure from lawmakers concerned about privacy. In a statement issued on July 12, House Majority Leader Dick Armey called on Attorney General Janet Reno and FBI Director Louis Freeh to "stop using this cybersnooping system until Fourth Amendment concerns are adequately addressed."

In addition, the House Judiciary Committee Subcommittee on the Constitution has scheduled a hearing on the matter for Monday, July 24. The ACLU has asked to submit testimony to the Committee.

The FBI has 20 business days to respond to the FOIA request. The ACLU is seeking a response on an expedited basis, the letter said, "because this information relates to impending policy decisions to which informed members of the public might contribute."

"If our request is denied in whole or part, we ask that you justify all deletions by reference to specific exemptions of the act," the ACLU letter concluded.

The ACLU's letter to the FBI follows.

July 14, 2000

Attention:
John Kelso Jr.
Federal Bureau of Investigation
Chief, FOI/PA Section, Rm. 6296 JEH
Washington, D.C. 20535-0001

Dear Mr. Kelso:

We are writing pursuant to the Freedom of Information Act (5 U.S.C. Sec. 552) to request all agency records including letters, correspondence, tape recordings, notes, data, memoranda, email, computer source and object code, technical manuals, technical specifications, or any other materials held by the Federal Bureau of Investigation regarding the following:

1. The computer system, software or device known as "Carnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers;
2. The computer system, software or device known as "Omnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers, and
3. The computer system, software or device known as "EtherPeek", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers.

We seek a waiver of fees associated with the fulfillment of this request for all search and processing fees, pursuant to Section 552(a)(4)(A)(ii)(II) of the Freedom of Information Act. Records are not sought for commercial use, and as a representative of the news media, the American Civil Liberties Foundation (ACLU Foundation) qualifies for a fee waiver under this provision of the FOIA. The organization meets the criterion laid out in *National Security Archive v. Department of Defense*, where a representative of the news media is defined as an entity that "gathers information of potential interest to a segment of the public" and "uses its editorial skills to turn raw materials into a distinct work, and distributes that work to an audience." 881 F.2d at 1387. The ACLU Foundation publishes newsletters, frequent press releases, news briefings, right to know handbooks, and other materials that are disseminated to the public. Its material is widely available to everyone including tax exempt organizations, not-for-profit groups, law students and faculty for no cost or for a nominal fee through its public education department. The ACLU Foundation disseminates information through publications available on-line at www.aclu.org as well.

In addition we request a fee waiver for duplication costs because disclosure of this information is in the public interest. It is likely to contribute significantly to the public understanding of the activities of the government. The ACLU Foundation is a nonprofit

501(c)3 research and education organization working to increase citizen participation in governance issues. The ACLU Foundation is making this request specifically for the public's enhanced understanding of lawfully authorized wiretapping, its relationship to constitutional guarantees of privacy as well as an understanding of global technological developments in wire and electronic networks that facilitate and expedite such wiretapping. The public's interest is particularly pertinent in light of advancing communications technology and the rapid growth of the World Wide Web. These developments have greatly increased the communications interconnectedness of all the countries in the world, especially technologically advanced nations like the US and the Netherlands.

We also seek expedited review of this FOIA request because this information relates to impending policy decisions to which informed members of the public might contribute. Timely public access to these materials is necessary to fully inform the public about the issues surrounding communications interception and related technological developments.

If our request is denied in whole or part, we ask that you justify all deletions by reference to specific exemptions of the act. We expect you to release all segregable portions of otherwise exempt material. We reserve the right to appeal your decision to withhold any information or to deny a waiver of fees.

We look forward to your reply within 20 business days, as the statute requires under Section 552(a)(6)(A)(I).

Thank you for your assistance.

Sincerely,

Barry Steinhardt, Esq.
On behalf of the ACLU Foundation

INDEX	JOIN	HOME	SEARCH	FEEDBACK
-------	------	------	--------	----------

Copyright 2000, The American Civil Liberties Union



American Civil Liberties Union
Freedom Network

ACLU Urges Congress to Put a Leash on "Carnivore" And Other Government Snoopware Programs

FOR IMMEDIATE RELEASE
Wednesday, July 12, 2000

WASHINGTON -- Law enforcement officials using new surveillance technologies online are racing far ahead of established privacy law and must be reined in, the American Civil Liberties Union said today.

In a letter sent to Charles T. Canady, R-FL, Chair of the Constitution Subcommittee of the House Judiciary Committee, and ranking member Melvin L. Watt, D-NC, the ACLU said that the unbridled uses of these technologies "cry out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age."

Specifically, the ACLU sharply criticized the FBI's new online wiretapping program, dubbed "Carnivore," that uses Internet Service Providers (ISPs) to intercept and analyze huge amounts of e-mail from suspects and non-suspects alike.

"It is high time that lawmakers put a leash on Carnivore and other government schemes that go way beyond what Congress authorized under the Electronic Communications Protection Act," said Laura W. Murphy, director of the ACLU's Washington National Office and an author of the letter.

Currently, law enforcement is required to "minimize" its interception of non-incriminating communications of a target of a wiretap order. But Carnivore does just the opposite, Murphy said, by sweeping in e-mails from innocent Internet users as well as the targeted suspect.

Barry Steinhardt, Associate Director of the ACLU and an author of the letter, said that implementing Carnivore "is comparable to allowing government agents to rip open Post Office mailbags and scan every piece of mail in search of one specific letter whose address they already know."

He also noted that while the system is plugged into the ISP, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.

The snoopware program first came to light during an April 6 hearing before the Constitution Subcommittee. The Carnivore system -- essentially a computer running specialized software-- is attached either when law enforcement has a court order permitting it to intercept in "real time" the contents of the electronic communications of a specific individual, or a trap-and-trace or pen register order allowing it to obtain the numbers related to communications from or to a specified target.

But "in the Internet context," the ACLU letter said, "these orders and certainly Carnivore likely involve ascertaining the suspect's e-mail address, as well as header information that may provide information regarding the content of the communication."

In urging Congress to accelerate its consideration of applying Fourth Amendment principles in the digital age, "we would be happy to work with the Subcommittee on drafting legislation that protects the privacy rights of Americans," the ACLU letter said.

The letter was signed by Murphy, Steinhardt, and Gregory T. Nojeim, legislative counsel with the ACLU's Washington National Office, who testified at the April 6 hearing.

In recent related developments, the ACLU has criticized other government surveillance schemes, including a global electronic surveillance system -- known by the code name of "Echelon" -- that is capturing satellite, microwave, cellular and fiber-optic communications worldwide.

The ACLU's letter on Carnivore is online at: <http://www.aclu.org/congress/071100a.html>.

For more information on the April 6 hearing, click <http://www.aclu.org/news/2000/n040600b.html>

For more information on "Echelon," go to <http://www.aclu.org/echelonwatch/>.

INDEX	JOIN	HOME	SEARCH	FEEDBACK
-------	------	------	--------	----------

Copyright 2000, The American Civil Liberties Union



In Congress

American Civil Liberties Union
Freedom Network

July 11, 2000

VIA FAX

Hon. Charles T. Canady, Chairman
Constitution Subcommittee of the
House Judiciary Committee
362 Ford House Office Bldg.
Washington, D.C. 20515-6220

and

Hon. Melvin L. Watt, Ranking Member
Constitution Subcommittee of the
House Judiciary Committee
362 Ford House Office Bldg.
Washington, D.C. 20515-6220

Dear Representatives Canady and Watt:

We are writing to you about the new FBI email surveillance system aptly named "Carnivore," which gives law enforcement extraordinary power to intercept and analyze huge volumes of email. The Carnivore system gives law enforcement email interception capabilities that were never contemplated when Congress passed the Electronic Communications Privacy Act (ECPA), codified in relevant part at 18 U.S.C. 2510-22 and 18 USC 3121-27. Carnivore raises new legal issues that cry out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age.

The existence of Carnivore first came to light in the April 6 testimony of Attorney Robert Corn-Revere to the Constitution Subcommittee. Its operation was further detailed in a report that appeared in today's Wall Street Journal (copy attached). According to these reports, the Carnivore system -- essentially a computer running specialized software -- is attached directly to an Internet Service Provider's (ISP) network. Carnivore is attached either when law enforcement has a Title III order from a court permitting it to intercept in real time the contents of the electronic communications of a specific individual, or a trap and trace or pen register order allowing it to obtain the "numbers" related to communications from or to a specified target.

But unlike the operation of a traditional a pen register, trap and trace device, or wiretap of a conventional phone line, Carnivore gives the FBI access to all traffic over the ISP's network, not just the communications to or from a particular target. Carnivore, which is capable of analyzing millions of messages per second, purportedly retains only the messages of the specified target, although this process takes place without scrutiny of either the ISP or a court.

Carnivore permits access to the email of every customer of an ISP and the email of every person who communicates with them. Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the "assurance" that the FBI will record only conversations of the specified target. This "trust us, we are the Government" approach is the antithesis of the procedures required under our the wiretapping laws. They authorize limited electronic surveillance of the communications of specified persons, usually conducted by means of specified communications devices. They place on the provider of the communications medium the

responsibility to separate the communications of persons authorized to be intercepted from other communications.

Currently, law enforcement is required to "minimize" its interception of non-incriminating communications of a target of a wiretap order. Carnivore is not a minimization tool. Instead, Carnivore maximizes law enforcement access to the communications of non-targets.

In his testimony to your subcommittee Mr. Corn-Revere described the experience of his client, an ISP that was required to install Carnivore when presented with a trap and trace order. He detailed his client's concerns that a trap and trace order in the context of the Internet revealed information that Congress did not contemplate when it authorized their limited use. In the traditional telephone context, those orders reveal nothing more than the numbers dialed to or from a single telephone line. In the Internet context, these orders and certainly Carnivore, likely involve ascertaining the suspect's e-mail address, as well as header information that may provide information regarding the content of the communication.

As we have stated previously, the ACLU does not believe that it is clear that the Government can serve an order on an Internet service provider and obtain the e-mail addresses of incoming and outgoing messages for a particular subscriber. Further, it is not clear whether law enforcement agents use or should use authority under the pen register statute to access a variety of data, including Internet Protocol addresses, dialup numbers and e-mail logs. We certainly do not believe that it is clear that law enforcement can install a super trap and trace device that access to such information for all of an ISP's subscribers.

In light of the new revelations about Carnivore, the ACLU urges the Subcommittee to accelerate its consideration of the application of the 4th Amendment in the digital age. Legislation should make it clear that law enforcement agents may not use devices that allow access to electronic communications involving only persons other than a specified target for which it has a proper order. Such legislation should make clear that a trap and trace order served on an ISP does not authorize access to the contents of any communication - including the subject line of a communication -- and that the ISP bears the burden of protecting the privacy of communications to which FBI access has not been granted.

We would be happy to work with the Subcommittee on drafting legislation that protects the privacy rights of Americans.

Sincerely,

Laura W. Murphy
Director, ACLU Washington National Office

Barry Steinhardt
Associate Director, ACLU

Gregory T. Nojeim
Legislative Counsel, ACLU Washington National Office

cc: Members of the Constitution Subcommittee of the House Judiciary Committee

[\[Legislative Archives\]](#) [\[106th Congress Issues\]](#) [\[Voters' Guide\]](#) [\[Congress Overview\]](#) [\[How to Use this Section\]](#)

INDEX	JOIN	HOME	SEARCH	FEEDBACK
-----------------------	----------------------	----------------------	------------------------	--------------------------

Copyright 1999, The American Civil Liberties Union

[Help](#) | [Contact Us](#) | [My Deja](#)

>> alt.privacy.spyware

>> Forum: [alt.privacy.spyware](#)

>> Thread: 'Carnivore' Won't Devour Cyber-Privacy

>> Message 11 of 1589

Save this thread

[back to search results](#)

Subject: Re: 'Carnivore' Won't Devour Cyber-Privacy

Date: 07/22/2000

Author: husky <cbminfo@digital.net>

<< previous in search · next in search >>

Message segment 2 of 2 - Get Previous Segment - Get All 2 Segments

If you give up your personal privacy, every other freedom will follow shortly. Though for my bucks, I say let carnivore loose. Whether carnivore does it's job or not has little to do with whether or not your health or credit records are safe. If you've posted your credit card anywhere on the web, chances are good it's no longer safe. And carnivore wouldn't have stopped that problem one way or the other. Health records? Somehow I can't see hospitals storing personal patient records on the web, but maybe transmitting them for short periods to other computers but zero storage on the web.

- > Fixing the relationship between Washington and Silicon Valley needs to be
- > a top priority for the next administration. The only people benefitting from
- > controversies like the one over Carnivore are terrorists, criminals and
- > rogue states.

The above has little to do with carnivore the above mentioned groups will always exploit the weaknesses of others to gain their ends.

Carnivore is just the current subject under scrutiny.

Don't do your criminal activity over the web, and you haven't any reason to worry about carnivore. Couldn't get any simpler.

<< previous in search · next in search >>

Subscribe to alt.privacy.spyware

Mail this message to a friend

[View original Usenet format](#)

Create a custom link to this message from your own Web site

Search Discussions	Search Discussions
Search only in	Search only in
Search in	Search in
Search	Search

deja Career
Center

Powered by
JobOptions.com
Early on Monday



Before you buy

DO IT HERE

JOB!

Help | Contact Us | My Deja

Home >> Discussions >> alt.comp.freeware

>> alt.comp.freeware

SEARCH>>

>> Forum: alt.comp.freeware
 >> Thread: British law would allow police to intercept e-mail
 >> Message 2 of 1589

Save this thread

back to search results

Subject: Re: British law would allow police to intercept e-mail

Date: 07/24/2000

Author: Taliesin2 <taliesin2@earthlink.net>

POST REPLY

<< previous in search · next in search >>

Message segment 1 of 2 - Get [Next Segment](#) - [Get All 2 Segments](#)

URGENT ACTION ITEM! Congress agrees to hold
 hearing on Monday in response to public outrage
 over FBI's e-mail spy scheme

=====

You are receiving this alert because you participated in
 DefendYourPrivacy.com's successful 1999 campaign against the
 FDIC's proposed Know Your Customer bank spying regulation. If
 you do not want to receive further updates, please use the
 unsubscribe directions at the end of this message.

=====

* Immediate action required: Help us Kill the
 Carnivore!

On July 14 we issued a press release about an FBI cybersnooping device code-named
 Carnivore, which can scan millions of e-mails per second. Because Carnivore has unlimited
 power to spy on almost everyone with an e-mail account, it may be the biggest threat to your
 digital
 privacy ever.

Almost immediately after the existence of this project was disclosed in a July 11 Wall Street
 Journal article, public outrage began to mount -- and now Congress has been pressured into
 holding hearings on Carnivore.

To capitalize on Monday's hearing before a House Judiciary Committee panel, we've launched
 a campaign to "Kill the Carnivore"!

Politicians on Capitol Hill may be planning to mollify the public by starting an "investigation" into
 the system, but that's not enough: We want to stop the Carnivore in its tracks and kill it --
 before it devours your privacy.

Please read this e-mail and "IMMEDIATELY" take the action below. Then forward this e-mail to
 friends, and ask them to do the same.

BACKGROUND:

Carnivore is a hardware-software device that the FBI secretly
 developed at its lab in Quantico, Va. Dubbed Carnivore because of its ability to find "the meat"
 among millions of e-mails, Carnivore scans every incoming and outgoing e-mail message on a
 network looking for telltale words or names, and saves those messages for later retrieval by

deja Career Center

- Job Search
- Post Resumes
- Career Tools
- For HR/Recruiters

and more!

Explore More

law enforcement. Carnivore can also track instant messages, visits to web sites, and Internet relay chat sessions.

The FBI admits that Carnivore will scan millions of e-mail messages from innocent people to find a tiny number of messages from people suspected of crimes. That's no different than if the FBI opened everyone's mail hoping to find a letter from a criminal, or listened in on everyone's phone calls just in case a crime was being discussed.

Though Carnivore's existence was just publicly revealed, the FBI has already installed the device at dozens of Internet Service Providers (ISPs) around the country, and claims it has used it "fewer than 50 times" so far. In many cases, the FBI keeps the device in a locked cage on the ISP's premises, with agents making daily visits to retrieve the captured data.

Many ISPs have refused to allow the FBI to install Carnivore, citing concerns that the privacy of all their customers could be violated. But earlier this year, a federal judge ruled against one such ISP, leaving it no choice but to allow the FBI access to its system.

Predictably, the FBI promises to limit surveillance to messages from suspected hackers, terrorists, or drug dealers. But considering that this is the same agency that quietly inserted "roving telephone tap" authority into federal law and illegally turned over confidential personnel files to the Clinton White House, you shouldn't be expected to trust it with your confidential e-mails.

But Carnivore is more than a threat to your ordinary e-mail correspondence -- it also gives government bureaucrats the ability to spy on your online banking transactions, because it has the ability to monitor all digital communications. The bottom line is that your privacy won't be protected as long as Carnivore is on the loose.

POST REPLY

<< [previous in search](#) · [next in search](#) >>

[Subscribe to alt.comp.freeware](#)

[Mail this message to a friend](#)

[View original Usenet format](#)

[Create a custom link to this message from your own Web site](#)

Search Discussions	For a more detailed search in Discussions go to PowerSearch
Search only in:	<input checked="" type="radio"/> All comp.freeware
	<input type="radio"/> All Open
Search for:	<input type="text" value="carnivore"/>
	<input type="button" value="Search"/>
Search	<input type="button" value="Submit"/> <input type="button" value="Advanced"/>

Copyright © 1995-2000 Deja.com, Inc. All rights reserved.

[Trademarks](#) · [Terms and Conditions of Use](#) · [Site Privacy Statement](#)

[Advertise With Us](#) | [About Deja.com](#) | [Careers @](#)

[Wolf Camera](#) · [Free Stuff@FreeShop](#) · [Tires.com](#) · [Deja e-centives](#) · [ELECTRONICS@SupremeVideo](#) · [Tire Rack.com](#) · [Coat of Arms](#) · [DeCOST](#)
[Search for Jobs!](#) Job Options: As Low as 2.9% Intro APR! Domain Registration! FREE Software! NEW Cars @ CarOrder

weapon is slow, silent, invisible, and men perceive it only by its consequences - by the gutted ruins and the moans of agony it leaves in its wake. The name of the weapon is: inflation.

- Ayn Rand, "Egalitarianism And Inflation," Philosophy: Who Needs It

ICQ: 9815080 **Disabled** Operator Taliesin_2 of #SacredNemeton on IRC PaganPaths

POST REPLY

[<< previous in search](#) - [next in search >>](#)

[Subscribe to all comp.freeware](#)

[Mail this message to a friend](#)

[View original Usenet format](#)

[Create a custom link to this message from your own Web site](#)

Search:	Ref: Deja.com Deja.com Deja.com Deja.com Deja.com
Discussions:	
Search for:	<input type="radio"/> all discussions
	<input type="radio"/> all discussions
Search on:	<input type="text"/>
	<input type="button" value="Search"/>
	<input type="button" value="Search"/> <input type="button" value="Search"/> <input type="button" value="discussions"/>

Copyright © 1995-2000 Deja.com, Inc. All rights reserved.

[Trademarks](#) - [Terms and Conditions of Use](#) - [Site Privacy Statement](#)

[Advertise With Us](#) | [About Deja.com](#) | [Careers @](#)

[Wolf Camera](#) - [Free Stuff@FreeShop](#) - [Tires.com](#) - [Deja e-cenives](#) [ELECTRONICS@SupremeVideo](#) - [TireRack.com](#) - [Cost+Pricing@eCOST](#)
[Search for Jobs!](#) [JobOptions](#) - [As Low as 2.9% Intro APR](#) - [Domain Registration](#) - [FREE Software](#) [NEWcars@carOrder](#)

Home
Custom Search
Dogpile Remote
Search at Home
Help with Syntax
MetaFind Search
Tell a Friend



DOGPILE

Web Metasearch Results

Lowest prices on the net for products and services

Home & Life • Collectibles • Travel • Small Business



Add ecommerce to your site

9-out-of-10 people prefer it to
thumb-twiddling.

Ask any question you can think of -
Free!

Buy books about "carnivore" at Amazon.com

Search for "carnivore" on Electric Library

Are you looking for:	Carnivorous Plants	Carnivores 2	Cherryhill Carnivorous	Carnivore Vietnam
	Carnivores In Ecosystems	California Carnivores	Carnivores II	Carnivores Game

Search engine: **Deja News** found 30 documents.

The query string sent was carnivore

Date	Subject	Forum	Author
07/24/2000	Re: CNN Story on FBI Carnivo	comp.security.firewal	David
07/24/2000	Re: British law would allow	alt.comp.freeware	Taliesin2
07/24/2000	Carnivore	fido7.moldova.interne	Adrian Oboroc
07/23/2000	CNN Story on FBI Carnivore	comp.security.firewal	Andrew P. Hende
07/23/2000	Re: CNN Story on FBI Carnivo	comp.security.firewal	Andrew P. Hende
07/23/2000	Re: Carnivore is a Violation	talk.politics.misc	Maximum Acid
07/22/2000	Re: 'Carnivore' Won't Devour	alt.security.pgp	News
07/22/2000	CARNIVORE, THE ELECTRONIC GE	alt.conspiracy	roninart
07/22/2000	CARNIVORE THE ELECTRONIC GES	alt.politics.election	roninart
07/22/2000	Re: CARNIVORE, THE ELECTRONI	alt.conspiracy	Terry Jameson
07/22/2000	Re: 'Carnivore' Won't Devour	alt.privacy.spyware	husky
07/22/2000	FBI's Carnivore Page	alt.privacy	An Metet
07/22/2000	CARNIVORE THE ELECTRONIC GES	alt.politics	roninart
07/23/2000	Re: Does anyone know about t	alt.folklore.urban	Lara Hopkins
07/22/2000	Carnivore is a Violation of	talk.politics.misc	Secret Squirrel
07/22/2000	Re: Who'se ISPs are being mo	austin.internet	D. Cook
07/22/2000	announce@lp.org: Urgent Acti	alt.law-enforcement	Mark2101
07/22/2000	Lebedev le carnivore	fr.soc.economie	KAGANOVITCH
07/22/2000	Does anyone know about the C	alt.folklore.urban	William B. Swea
07/22/2000	Does anyone know about the C	alt.folklore.urban	William B. Swea
07/22/2000	Kill It!	alt.religion.w-w-chur	Janice Matchett
07/22/2000	Kill It!	alt.religion.w-w-chur	Janice Matchett
07/22/2000	Carnivore	talk.politics.guns	Silverdahl
07/22/2000	Carnivore	talk.politics.guns	Silverdahl
07/22/2000	Seems Clinton's and Reno's C	3dfx.products.voodoo5	Greg S. Trouw
07/22/2000	Re: announce@lp.org: Release	talk.politics.guns	rcain.nospam

07/22/2000	Re: announce@lp.org: Release	talk.politics.guns	rcain.nospam
07/22/2000	Re: Carnivore	talk.politics.guns	Cuchulain Libby
07/22/2000	Can carnivore be used to pre	alt.privacy	withheld
07/22/2000	Re: Can carnivore be used to	alt.privacy	Norm G.
07/22/2000	Re: Can carnivore be used to	alt.privacy	jungle

Search engine: AltaVista's Usenet Search found 100 documents.The query string sent was +carnivore

Date	Subject	Forum	Author
30 Jun	<u>Nutritional Sources?</u> <u>Vegan, Vegetarian Vs</u> <u>Carnivore</u>	yemenmocha@my- deja.com	alt.animals.ethics.veg...
09 Jul	<u>FA: OOP Carnivore</u> <u>and Rigor Mortis CDs</u>	Michael Siciliano	alt.rock-n-roll.metal
11 Jul	<u>FBI's Carnivore</u>	An Metet	alt.privacy.anon-server
11 Jul	<u>More on FBI's</u> <u>Carnivore</u>	An Metet	alt.privacy
11 Jul	<u>More Info On</u> <u>Carnivore, The Wire</u> <u>the FBI Have On Your</u> <u>ISP</u>	OsioniusX	alt.fan.cult-dead-cow
11 Jul	<u>Carnivore</u>	Glen Harman	news.admin.net-abuse.e...
11 Jul	<u>URGENT--- FBI's</u> <u>Carnivore may be on</u> <u>your ISP!</u> <u>Carnivore Eats Your</u> <u>Privacy</u>	Lazyike	rec.drugs.misc
		11 Jul	3 <u>Discordia SCC</u> (alt.discordia.scc)
11 Jul	<u>RE:CARNIVORE</u>	Anonymous	alt.privacy
11 Jul	<u>Big Brother's</u> <u>carnivore program*-*</u>	Fred	alt.privacy.anon-server
11 Jul	<u>OT - Superfast system</u> <u>called 'Carnivore'</u> <u>searches e-mails for</u> <u>messages</u>	Ronald Gillen	soc.culture.baltics
11 Jul	<u>FBI's CARNIVORE</u> <u>system</u>	Jose Vellancamp, Esquire	alt.drugs.pot
11 Jul	<u>Interesting Editorial</u> <u>on Carnivore</u>	the Pull	alt.fan.cult-dead-cow
11 Jul	<u>Carnivore Letter</u> <u>Printed in Entirety</u>	the Pull	alt.fan.cult-dead-cow
11 Jul	<u>Carnivore in</u> <u>nyc.transit means</u> <u>no.privacy!</u>	No User	nyc.transit
12 Jul	<u>The Emeraude Project,</u> <u>French</u> <u>Carnivore+Echelon</u>	nobody@nowhere.com	alt.privacy.anon-server
11 Jul	<u>Carnivore: Who Cares</u> <u>...ZZZZZZZZ</u>	Dan	alt.privacy.anon-server
12 Jul	<u>ACLU: Law Needs</u> <u>'Carnivore' Fix</u>	Viviane Lerner	flora.mai-not

- 'Carnivore' Fix**
- 12 Jul [Carnivore Causing concern](#) Jeremy Compton bit.listserv.cloaks-da...
- 12 Jul [FBI Big Brother Carnivore + Privacy Resources](#) E Right alt.politics.bush

There is 1 search engine left to be searched. For more results, click below.

Next Set of Search Engines

Are you looking for:

Carnivorous Plants	Carnivores 2	Cherryhill Carnivorous	Carnivore Vietnam
Carnivores In Ecosystems	California Carnivores	Carnivores II	Carnivores Game

Buy books about "carnivore" at [Amazon.com](#)

Search for "carnivore" on [Electric Library](#)




THIS IS HOW CUSTOMERS USED TO FIND YOU.

DOGPILE SEARCH GEOGRAPHIC SEARCH

carnivore

Fetch

- ☐ Web Metasearch ☐ Web Catalog ☒ Usenet ☐ Newscrawler ☐ BizNews ☐ Ftp
- ☐ Stock Quotes ☐ Jobs/Careers ☐ Weather ☐ Auctions ☒ Images 
- ☐ Yellow Pages ☐ White Pages ☐ Maps ☐ Audio/MP3

Text & Webinator Copyright (C) 1997 THUNDERSTONE - EPI, Inc.

NEWS

BUSINESS

POLITICS

WIRE SERVICE

CULTURE

TECHNOLOGY

TOP STORIES

Telecoms Miffed at FBI Meddling

by Declan McCullagh

3:00 a.m. Jul. 8, 2000 PDT

A telecommunications trade association this week criticized a recent FBI move to thwart the \$5.5 billion sale of ISP Verio to a Japanese firm.

The FBI's objections that the Fed agency may not be able to conduct the kind of Internet surveillance it desires are specious, said the Computer and Communications Industry Association.

Everybody's got issues in Politics
More Funding for FBI Snooping

"In taking this action the FBI runs the serious risk of frustrating the openness of Internet communications, infringing our civil liberties, and damaging our relations with important trading partners," said Ed Black, president of the CCIA. The groups' members include AT&T, Nortel, Nokia, and NTT America, the Japanese company which hopes to purchase Verio.

Last year, the FBI unsuccessfully asked the Internet Engineering Task Force to build wiretap capabilities into protocols. FBI Director Louis Freeh has, in the past, asked Congress for domestic controls on data-scrambling encryption products and successfully pressed for a "digital telephony" law that requires telephone companies to ensure that their networks are able to be tapped by the Feds.

Anti-anonymity: If you criticize a Pennsylvania judge online, be warned: You may not be as anonymous as you thought.

Thin-skinned Superior Court Judge Joan Orie Melvin in early 1999 sued over a dozen "John Does" that she suspected of posting messages on a muckraking site devoted to Pittsburgh politics.

A judge who recently heard arguments in Melvin's case will decide whether or not to unmask the folks who participated in the "Grant Street 99" site, according to an article in the *Pittsburgh Tribune-Review*.

The ACLU is defending the John Does, including one who reportedly alleged that Judge Melvin was engaged in surreptitious and -- if true -- unlawful partisan political activity.

Bill Joy a Killjoy? An article on the website of the conservative *National Review* takes aim at Bill Joy of Sun Microsystems, who recently raised eyebrows when he warned of the dangers of unregulated technology.

Authors Glenn Reynolds and Dave Kopel said Joy's article, published earlier this year in *Wired Magazine*, is an example of "neo-Luddite sentiment."

"More generally, Luddite intellectuals are successfully propagating 'the precautionary principle,' which states that we should never try anything new unless we are certain that it is absolutely safe... Even worse, 'relinquishment' would probably accelerate the progress of destructive nanotechnology. In a world where nanotechnology is outlawed, outlaws would have an additional incentive to develop nanotechnology," the *National Review* authors wrote.

Upcoming events: Two U.S. senators are holding a briefing on medical and genetic privacy on

July 14. The event, sponsored by the Forum on Technology Innovation is scheduled for 12:15 p.m. in room 325 of the Russell Senate office building... The Freedom Forum is releasing its state of the First Amendment survey on July 13 at 9 am... A federal online "child protection" commission meets July 20 in Richmond.

Related Wired Links:

ICANN Gets Mixed Review

Jul. 7, 2000

Oracle's Hot Summertime Fund

Jul. 1, 2000

Feds' Hands Caught in Cookie Jar

Jun. 30, 2000

How Congressional Cookies Crumble

Jun. 30, 2000

McCain Renews Porn-Filter Push

Jun. 28, 2000

'Twas Oracle That Spied on MS

Jun. 28, 2000

DOJ's Got the Antitrust Itch

Jun. 28, 2000

Copyright © 1994-2000 Wired Digital Inc. All rights reserved.